FIG. 1

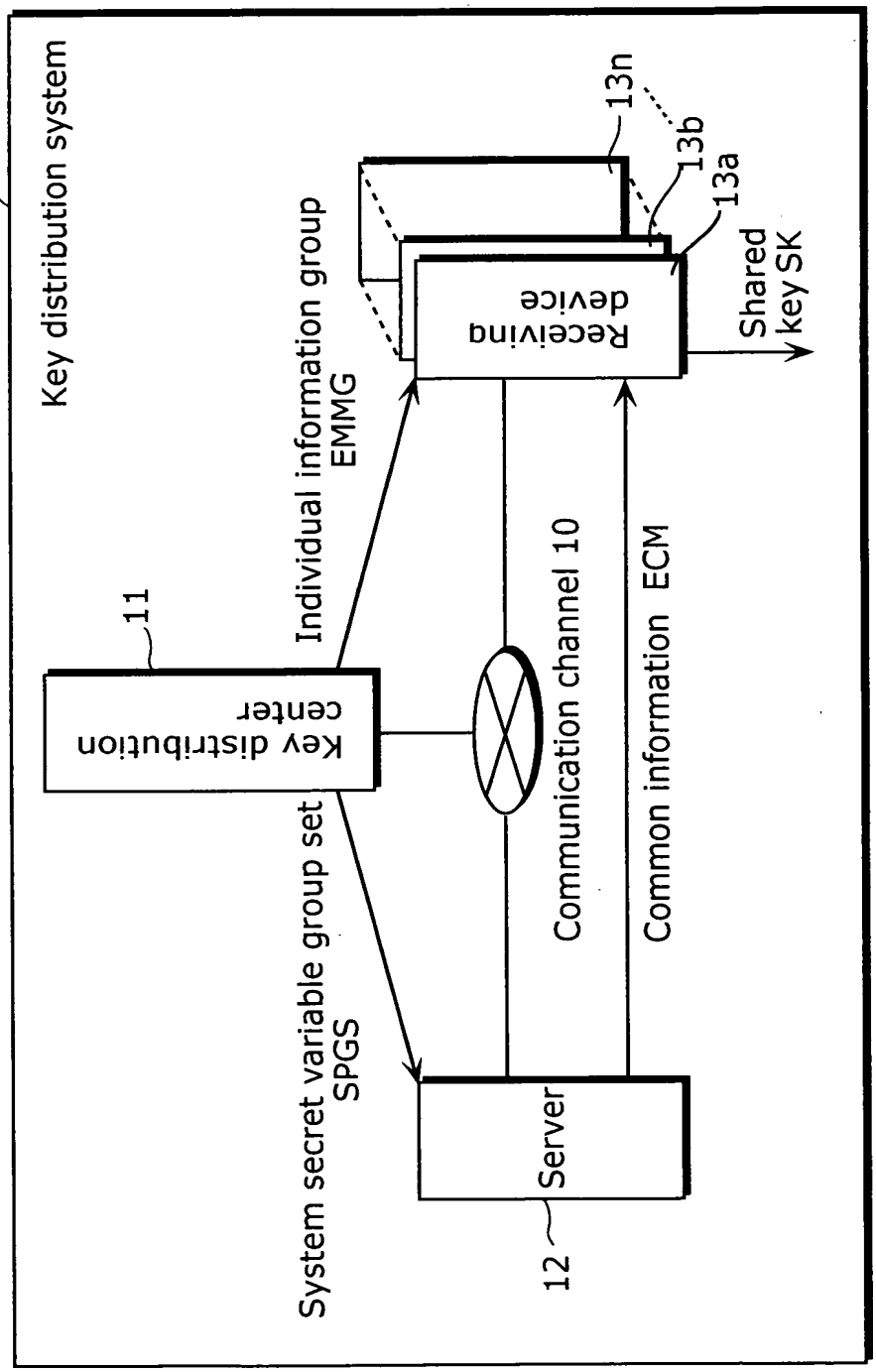

1
Key distribution system
11
Key distribution center
12
Server
13n
13b
13a
Receiving device
Shared key SK
Individual information group EMMG
System secret variable group set SPGS
Communication channel 10
Common information ECM

FIG. 2

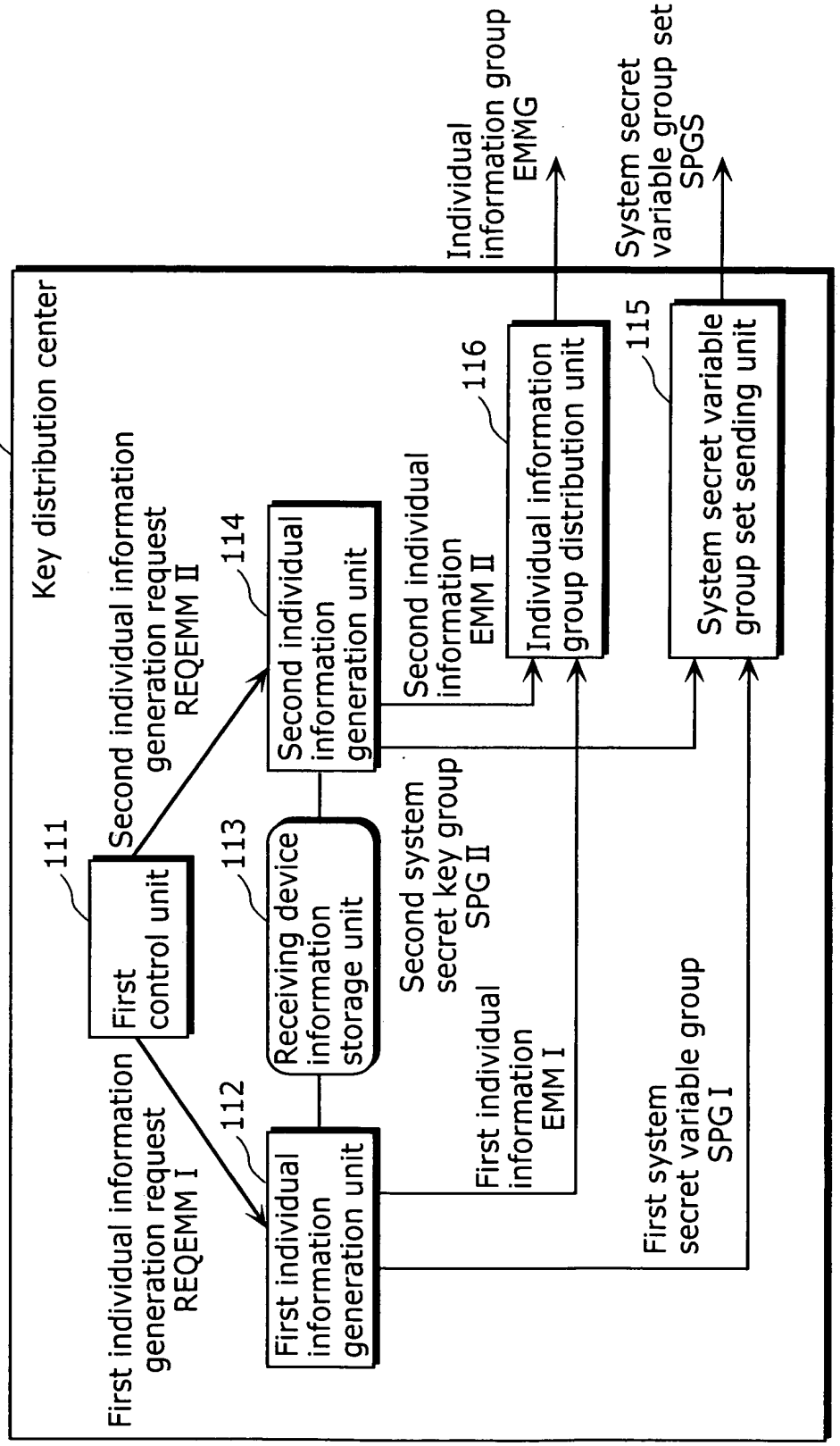

11
Key distribution center
111
First control unit
112
First individual information generation unit
113
Receiving device information storage unit
114
Second individual information generation unit
115
System secret variable group set sending unit
116
Individual information group distribution unit
First individual information generation request REQEMM I
Second individual information generation request REQEMM II
First individual information EMM I
Second individual information EMM II
Second system secret key group SPG II
First system secret variable group SPG I
Individual information group EMMG
System secret variable group set SPGS

FIG. 3

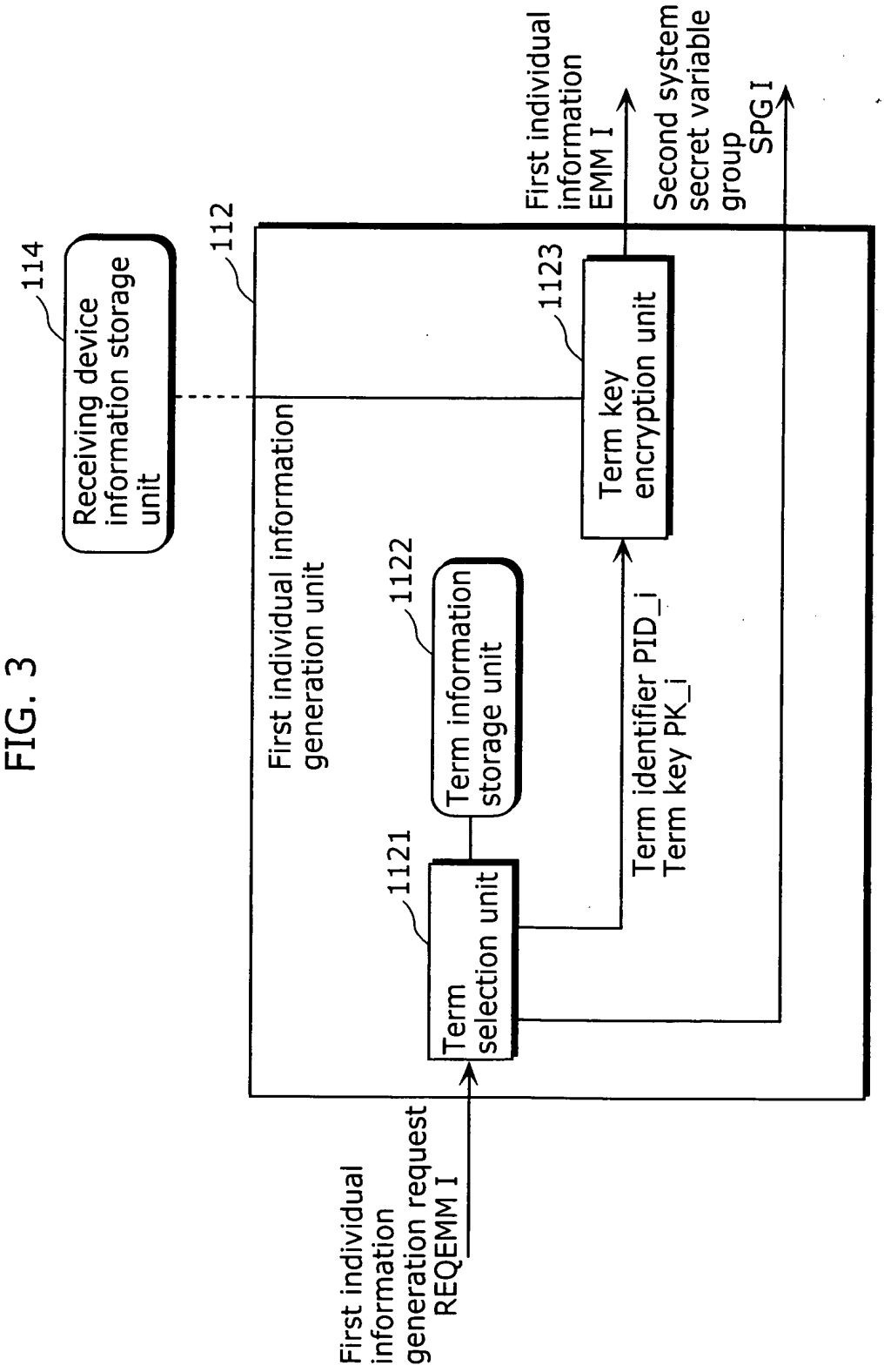

First individual information generation request REQEMM I
Receiving device information storage unit
114
112
First individual information generation unit
Term selection unit
1121
Term information storage unit
1122
Term key encryption unit
1123
Term identifier PID_i
Term key PK_i
First individual information EMM I
Second system secret variable group SPG I

FIG. 4

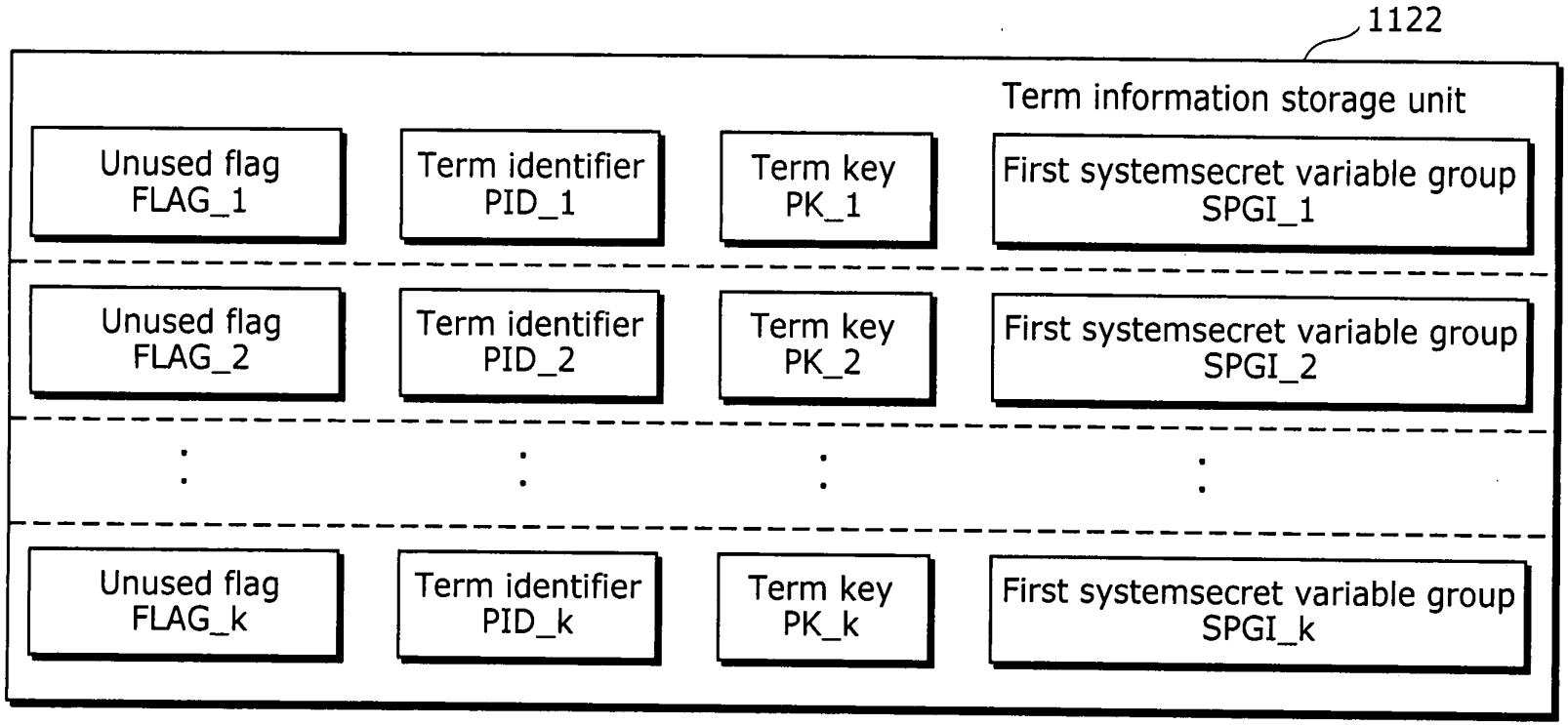

1122
Term information storage unit
Unused flag FLAG_1
Term identifier PID_1
Term key PK_1
First systemsecret variable group SPGI_1
Unused flag FLAG_2
Term identifier PID_2
Term key PK_2
First systemsecret variable group SPGI_2
Unused flag FLAG_k
Term identifier PID_k
Term key PK_k
First systemsecret variable group SPGI_k

FIG. 5

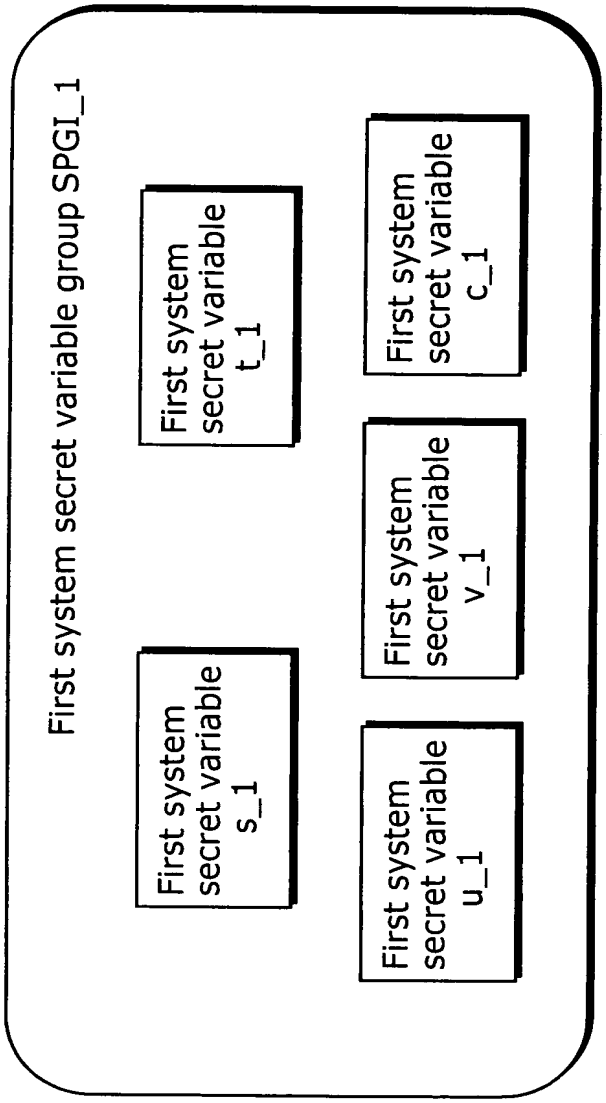

First system secret variable group SPGI_1
First system secret variable s_1
First system secret variable t_1
First system secret variable u_1
First system secret variable v_1
First system secret variable c_1

FIG. 6

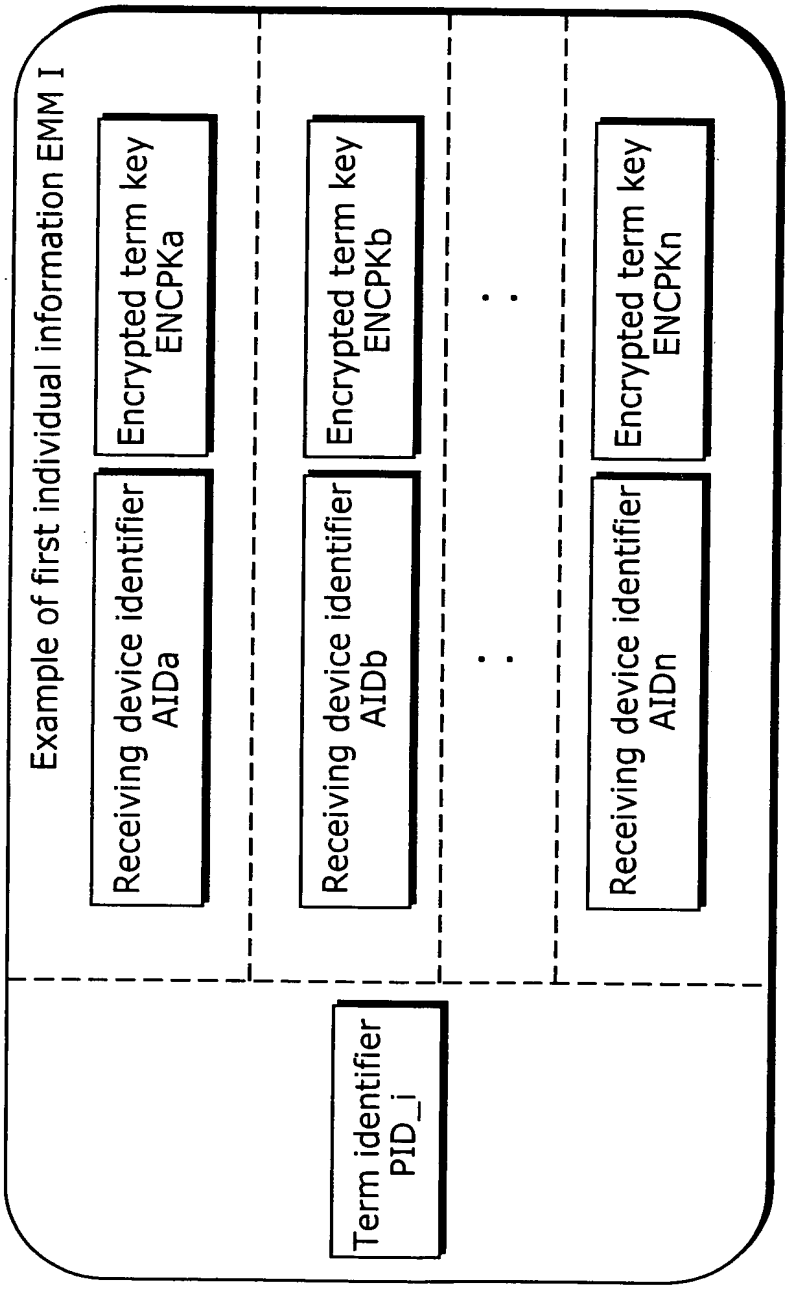

Example of first individual information EMM I
Term identifier PID_i
Receiving device identifier AIDa
Encrypted term key ENCPKa
Receiving device identifier AIDb
Encrypted term key ENCPKb
Receiving device identifier AIDn
Encrypted term key ENCPKn

FIG. 7

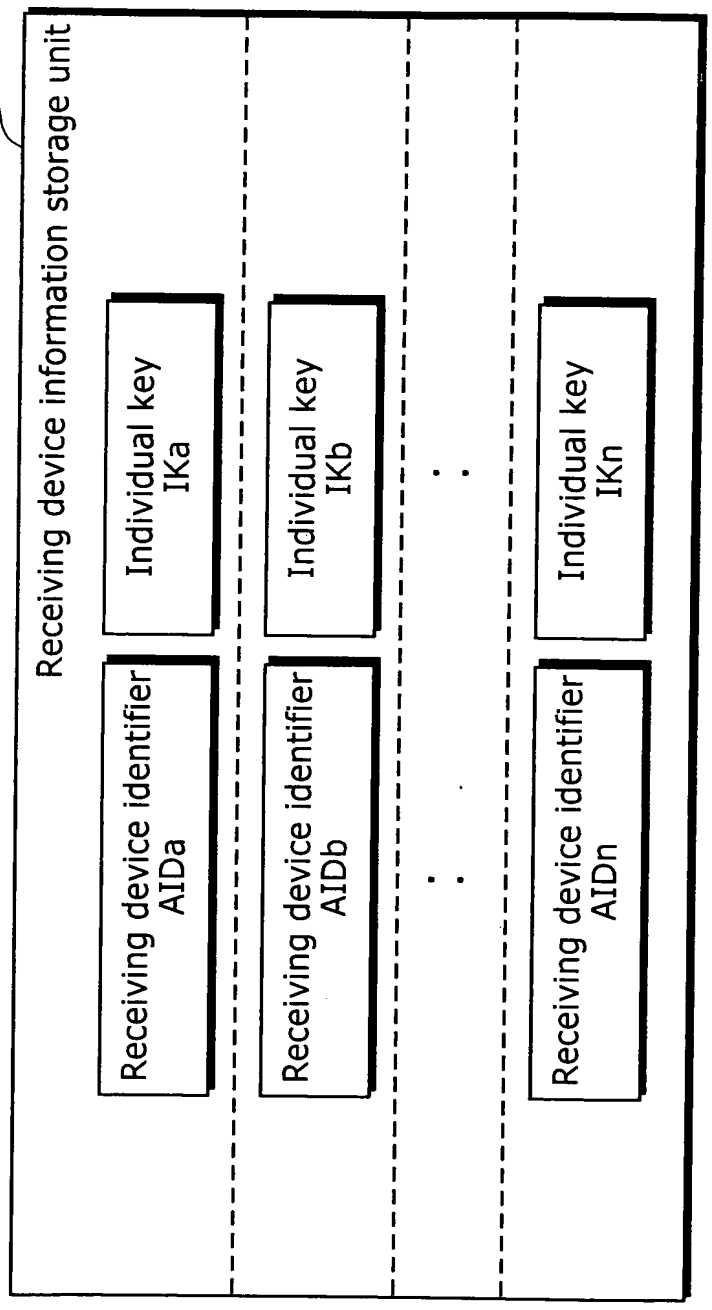

113
Receiving device information storage unit
Receiving device identifier AIDa
Individual key IKa
Receiving device identifier AIDb
Individual key IKb
Receiving device identifier AIDn
Individual key IKn

FIG. 8

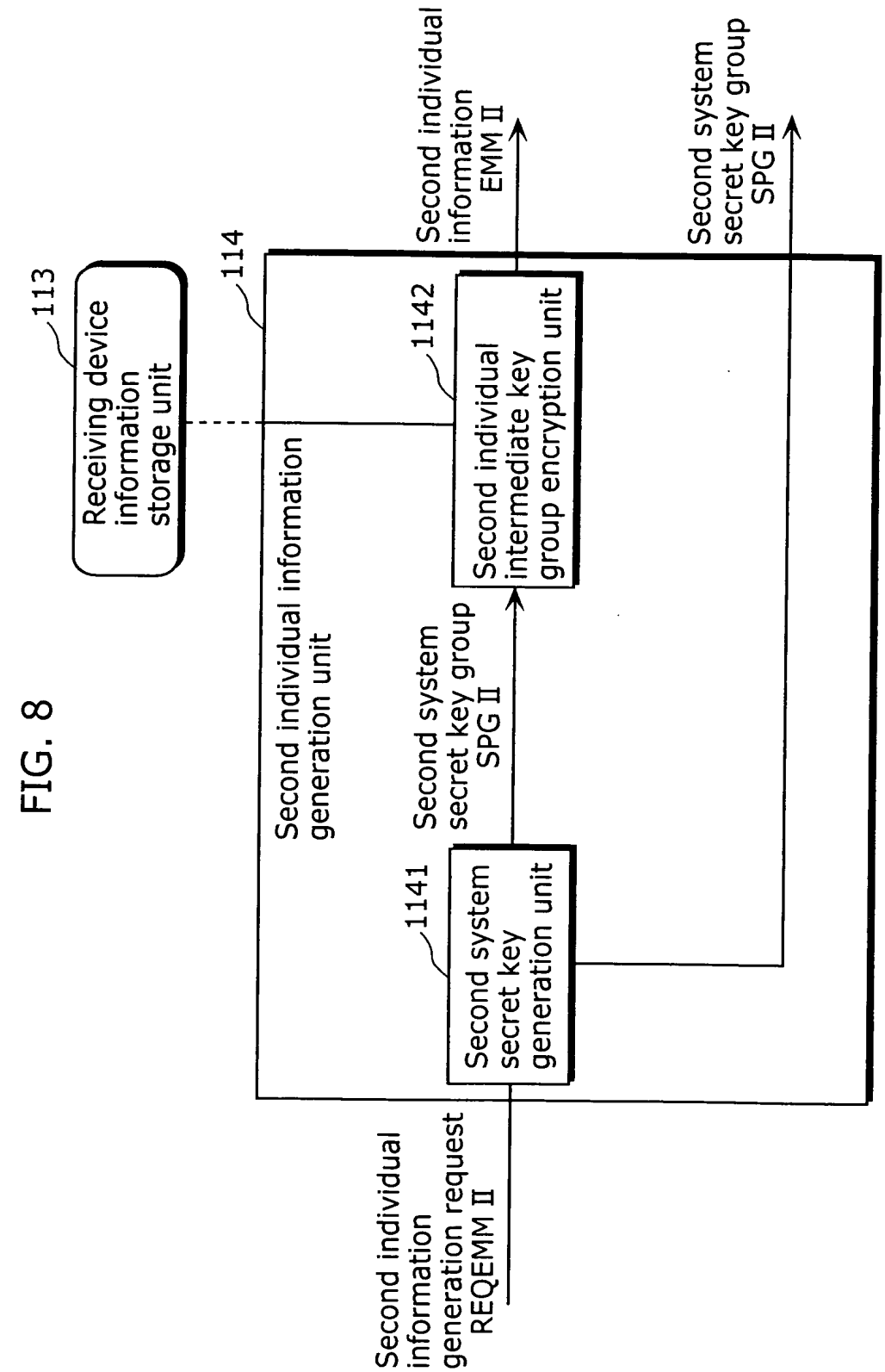

113
Receiving device information storage unit
114
Second individual information generation unit
1141
Second system secret key generation unit
1142
Second individual intermediate key group encryption unit
Second individual information generation request REQEMM II
Second system secret key group SPG II
Second individual information EMM II
Second system secret key group SPG II

FIG. 9

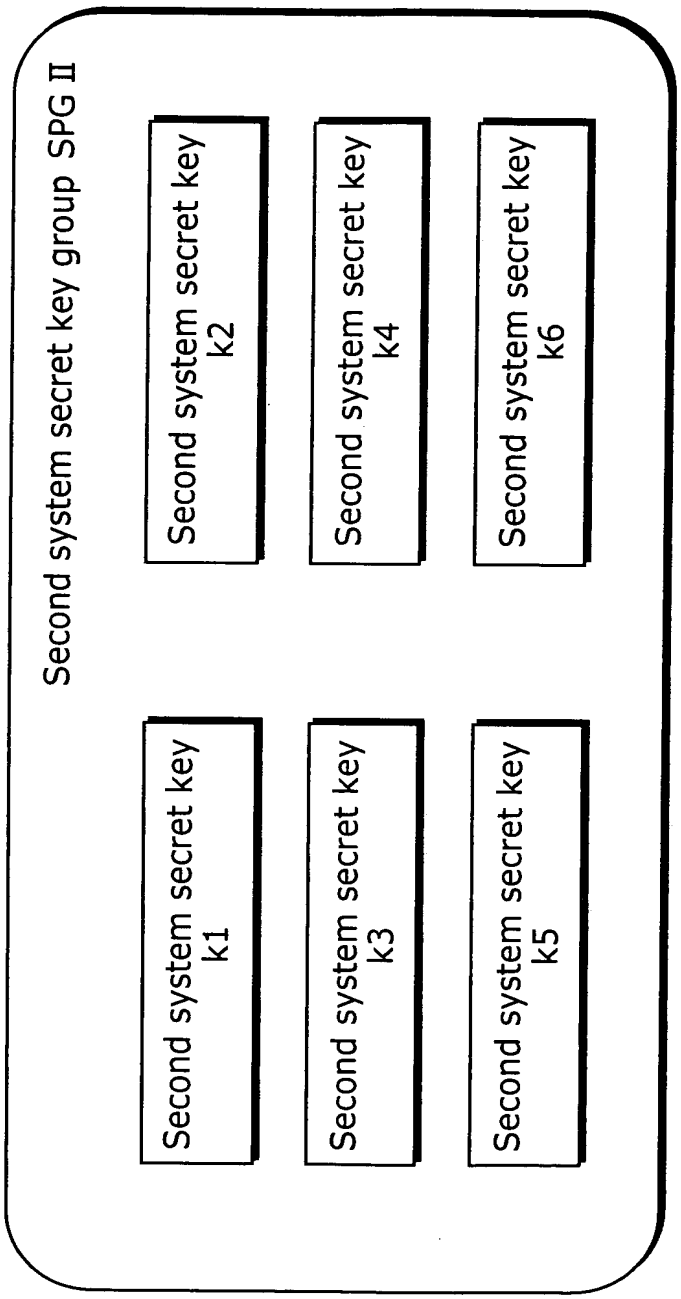

Second system secret key group SPG II
Second system secret key k2
Second system secret key k4
Second system secret key k6
Second system secret key k1
Second system secret key k3
Second system secret key k5

FIG. 10

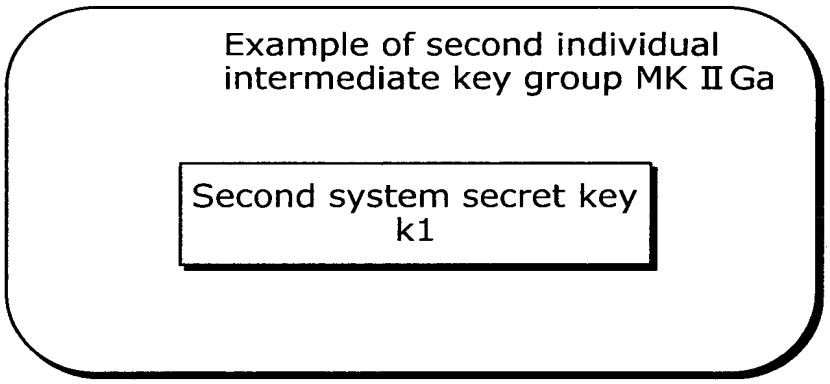

Example of second individual intermediate key group MK IIGa
Second system secret key k1

FIG. 11

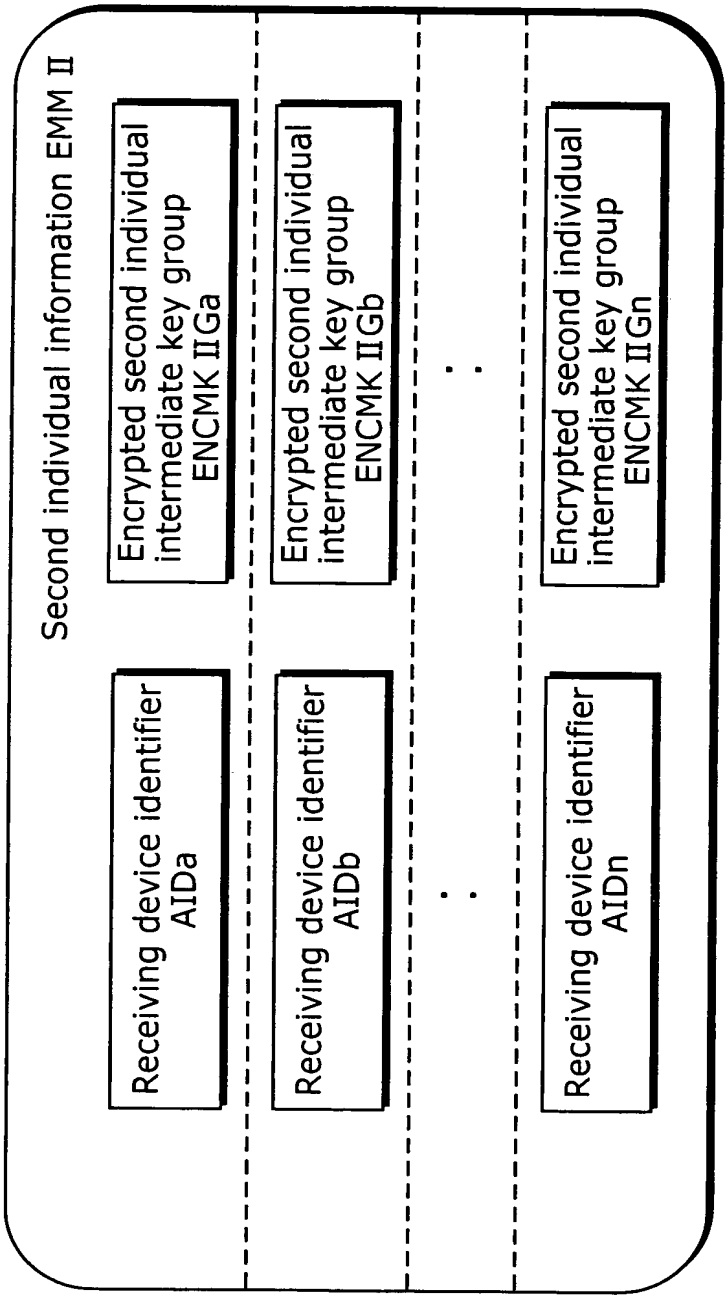

Second individual information EMM II
Receiving device identifier AIDa
Encrypted second individual intermediate key group ENCMK IIGa
Receiving device identifier AIDb
Encrypted second individual intermediate key group ENCMK IIGb
Receiving device identifier AIDn
Encrypted second individual intermediate key group ENCMK IIGn

FIG. 12

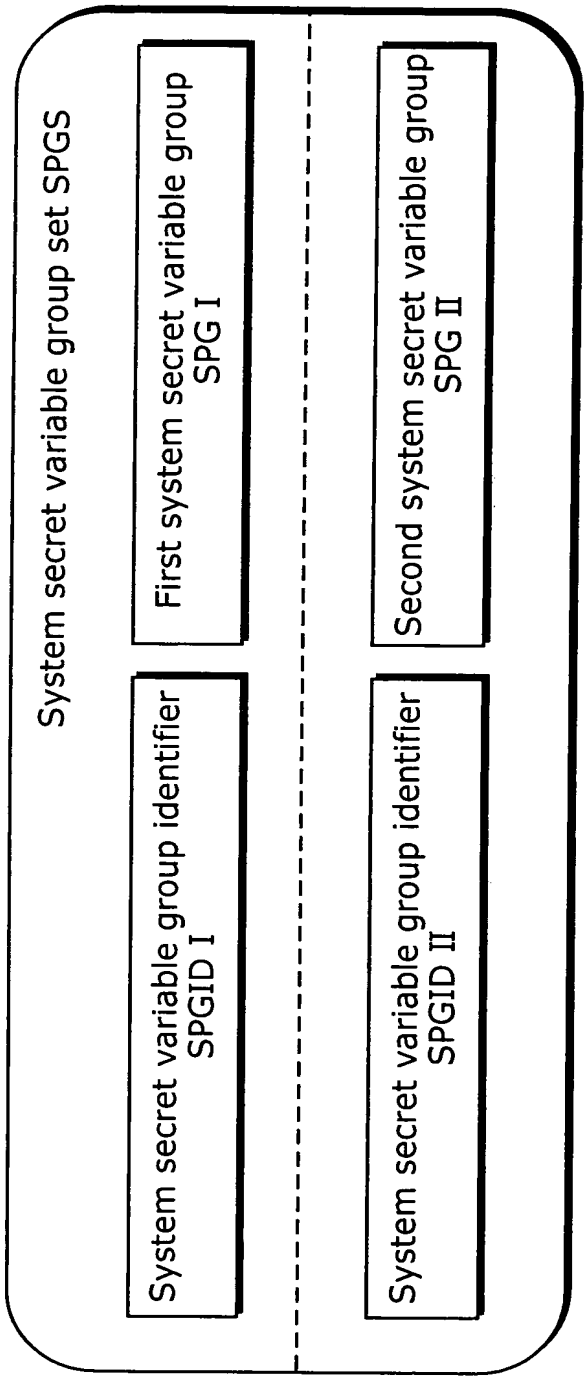

System secret variable group set SPGS
First system secret variable group SPG I
Second system secret variable group SPG II
System secret variable group identifier SPGID I
System secret variable group identifier SPGID II

FIG. 13

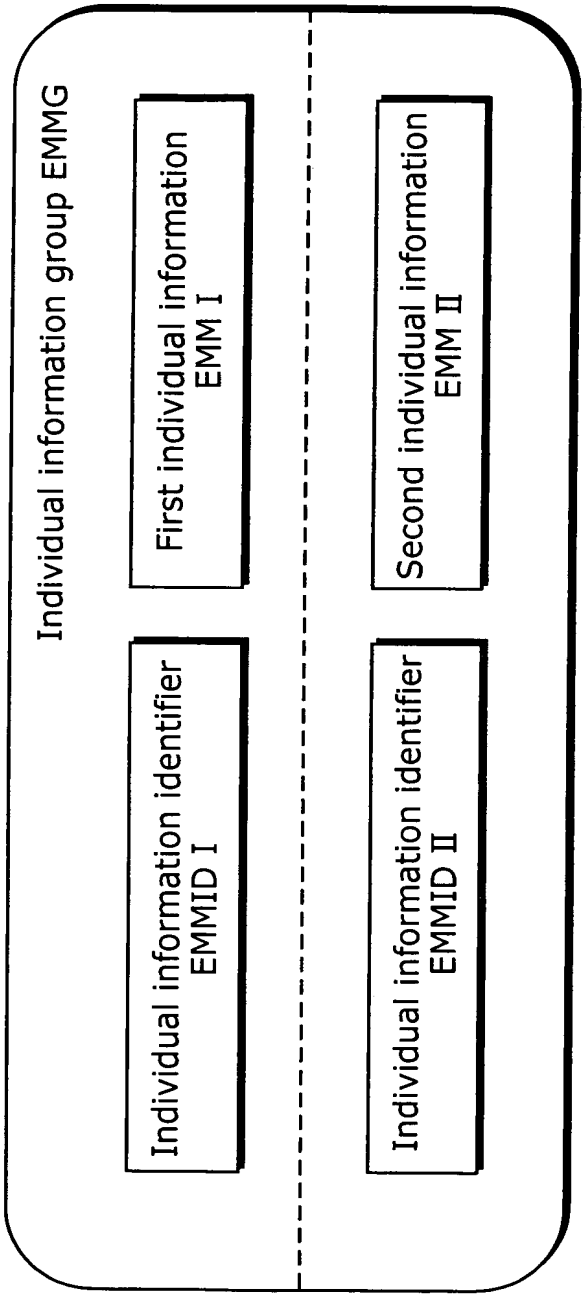

Individual information group EMMG
Individual information identifier EMMID I
First individual information EMM I
Individual information identifier EMMID II
Second individual information EMM II

FIG. 14

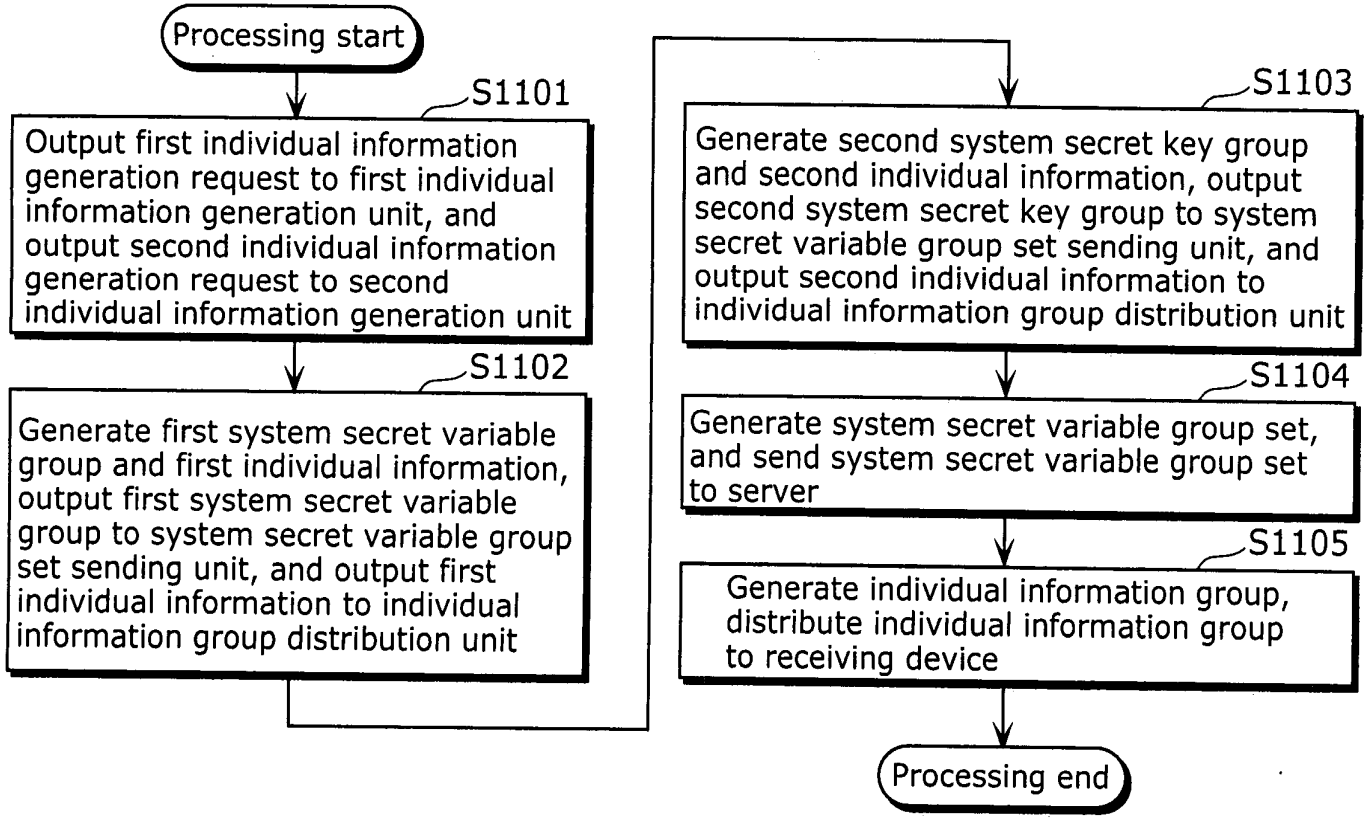

Processing start
S1101
Output first individual information generation request to first individual information generation unit, and output second individual information generation request to second individual information generation unit
S1102
Generate first system secret variable group and first individual information, output first system secret variable group to system secret variable group set sending unit, and output first individual information to individual information group distribution unit
S1103
Generate second system secret key group and second individual information, output second system secret key group to system secret variable group set sending unit, and output second individual information to individual information group distribution unit
S1104
Generate system secret variable group set, and send system secret variable group set to server
S1105
Generate individual information group, distribute individual information group to receiving device
Processing end

FIG. 15

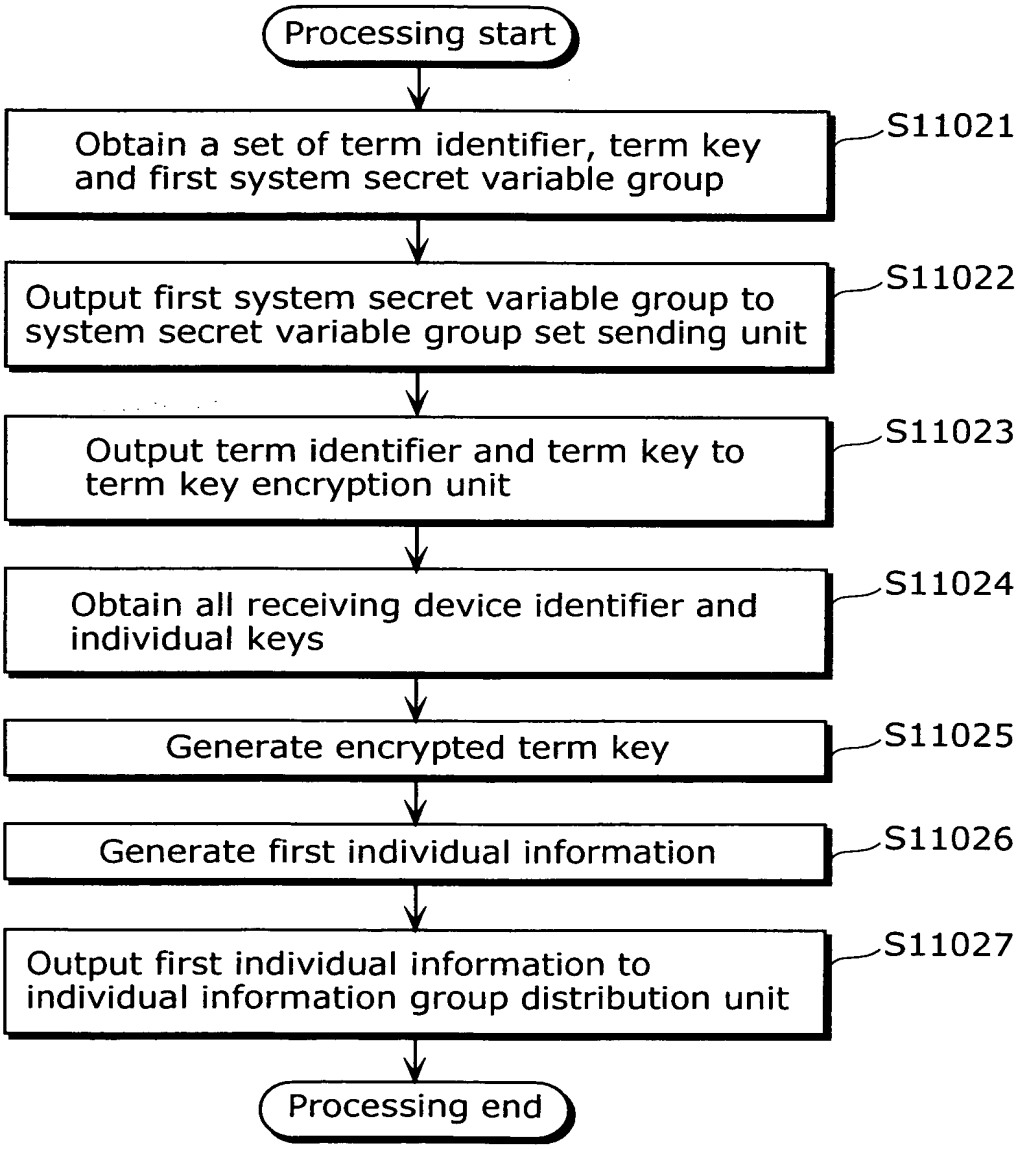

Processing start
Obtain a set of term identifier, term key and first system secret variable group
S11021
Output first system secret variable group to system secret variable group set sending unit
S11022
Output term identifier and term key to term key encryption unit
S11023
Obtain all receiving device identifier and individual keys
S11024
Generate encrypted term key
S11025
Generate first individual information
S11026
Output first individual information to individual information group distribution unit
S11027
Processing end

FIG. 16

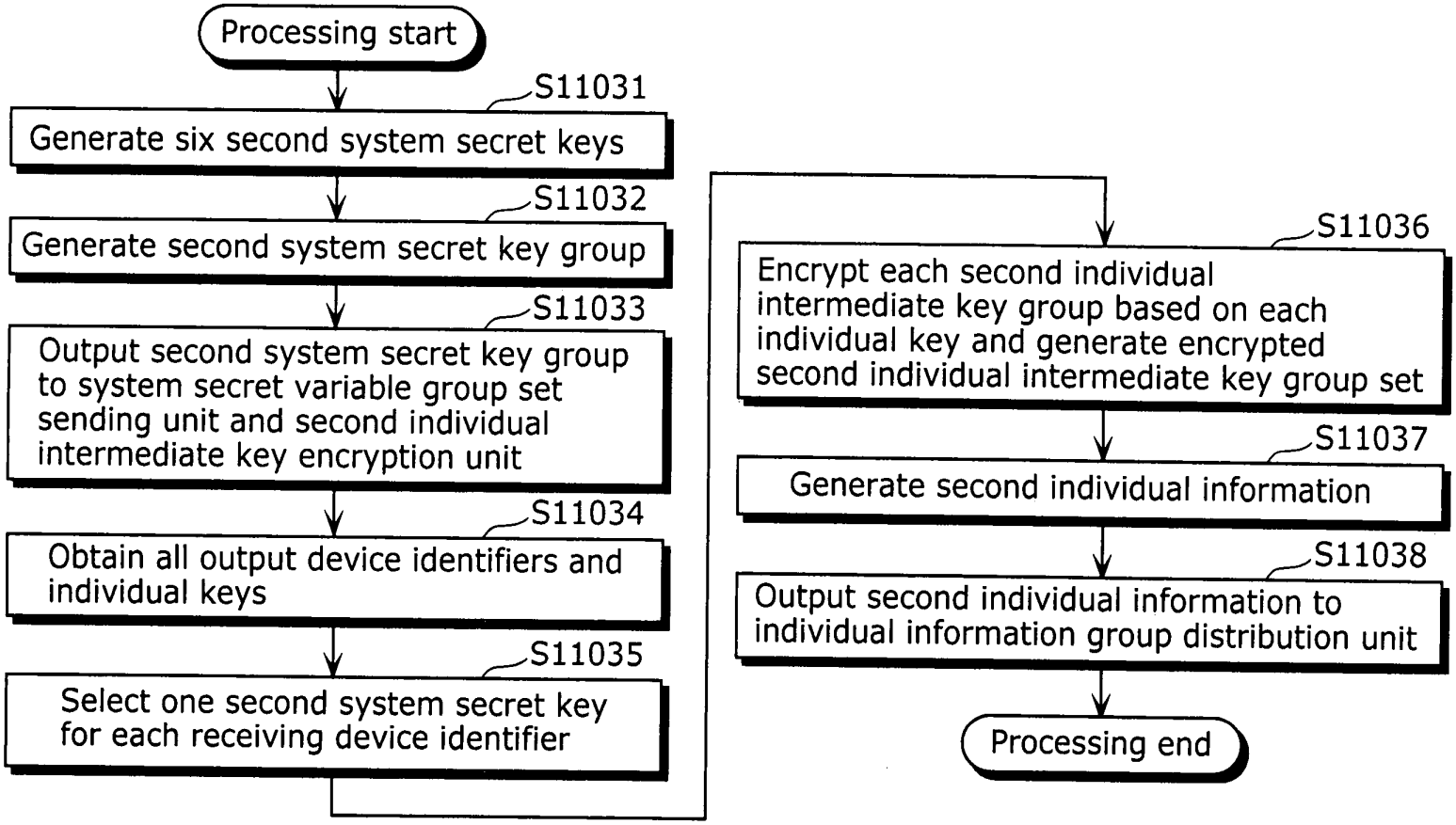

Processing start
S11031
Generate six second system secret keys
S11032
Generate second system secret key group
S11033
Output second system secret key group to system secret variable group set sending unit and second individual intermediate key encryption unit
S11034
Obtain all output device identifiers and individual keys
S11035
Select one second system secret key for each receiving device identifier
S11036
Encrypt each second individual intermediate key group based on each individual key and generate encrypted second individual intermediate key group set
S11037
Generate second individual information
S11038
Output second individual information to individual information group distribution unit
Processing end

FIG. 17

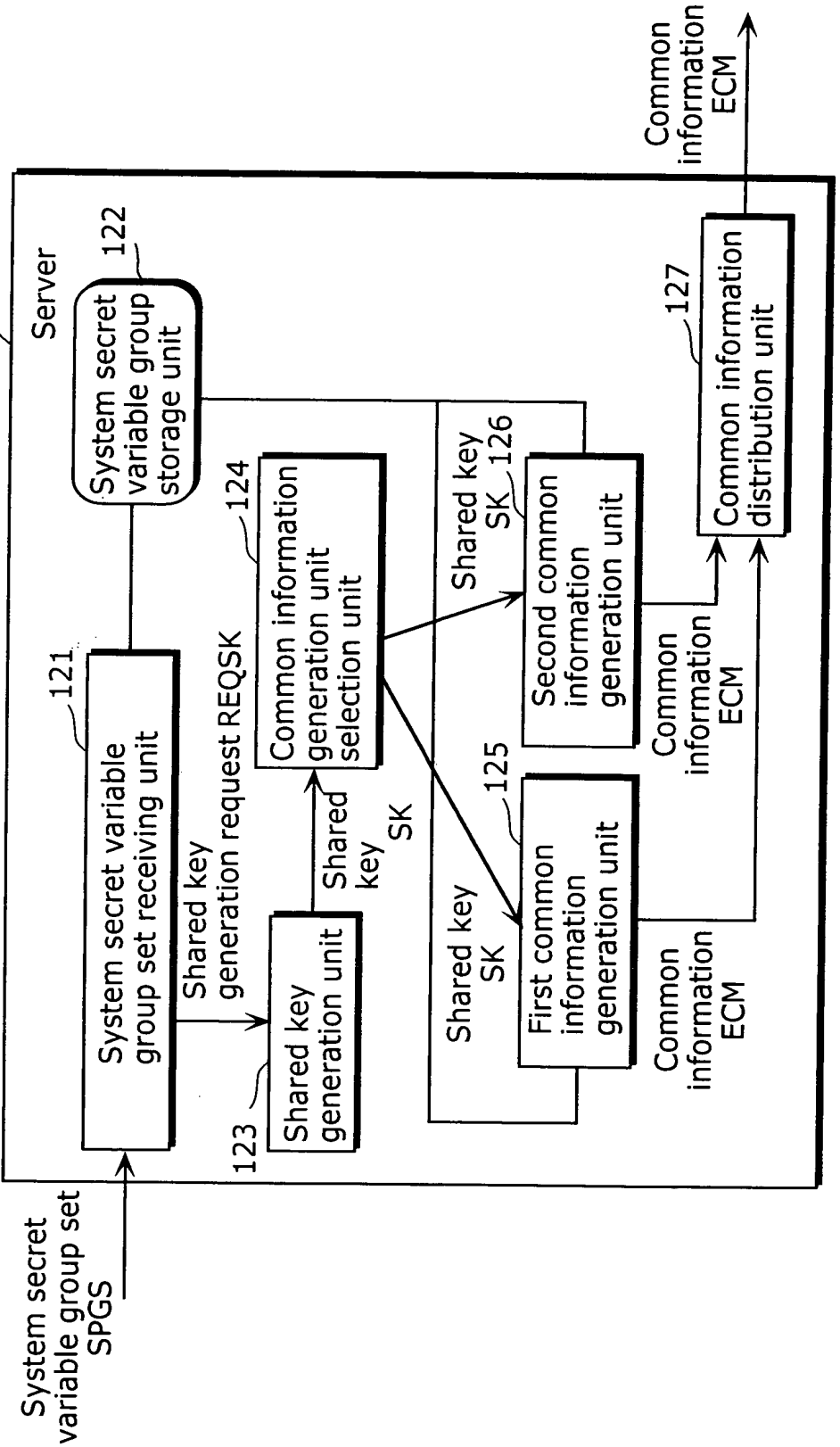

12
Server
122
System secret variable group storage unit
121
System secret variable group set receiving unit
Shared key generation request REQSK
123
Shared key generation unit
Shared key SK
124
Common information generation unit selection unit
Shared key SK
125
First common information generation unit
Shared key SK
126
Second common information generation unit
127
Common information distribution unit
Common information ECM
Common information ECM
Common information ECM
System secret variable group set SPGS

FIG. 18

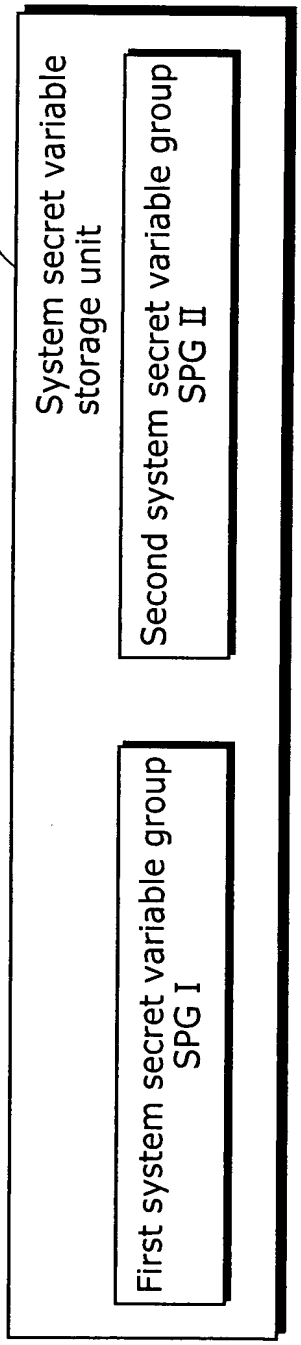

122
System secret variable storage unit
Second system secret variable group SPG II
First system secret variable group SPG I

FIG. 19

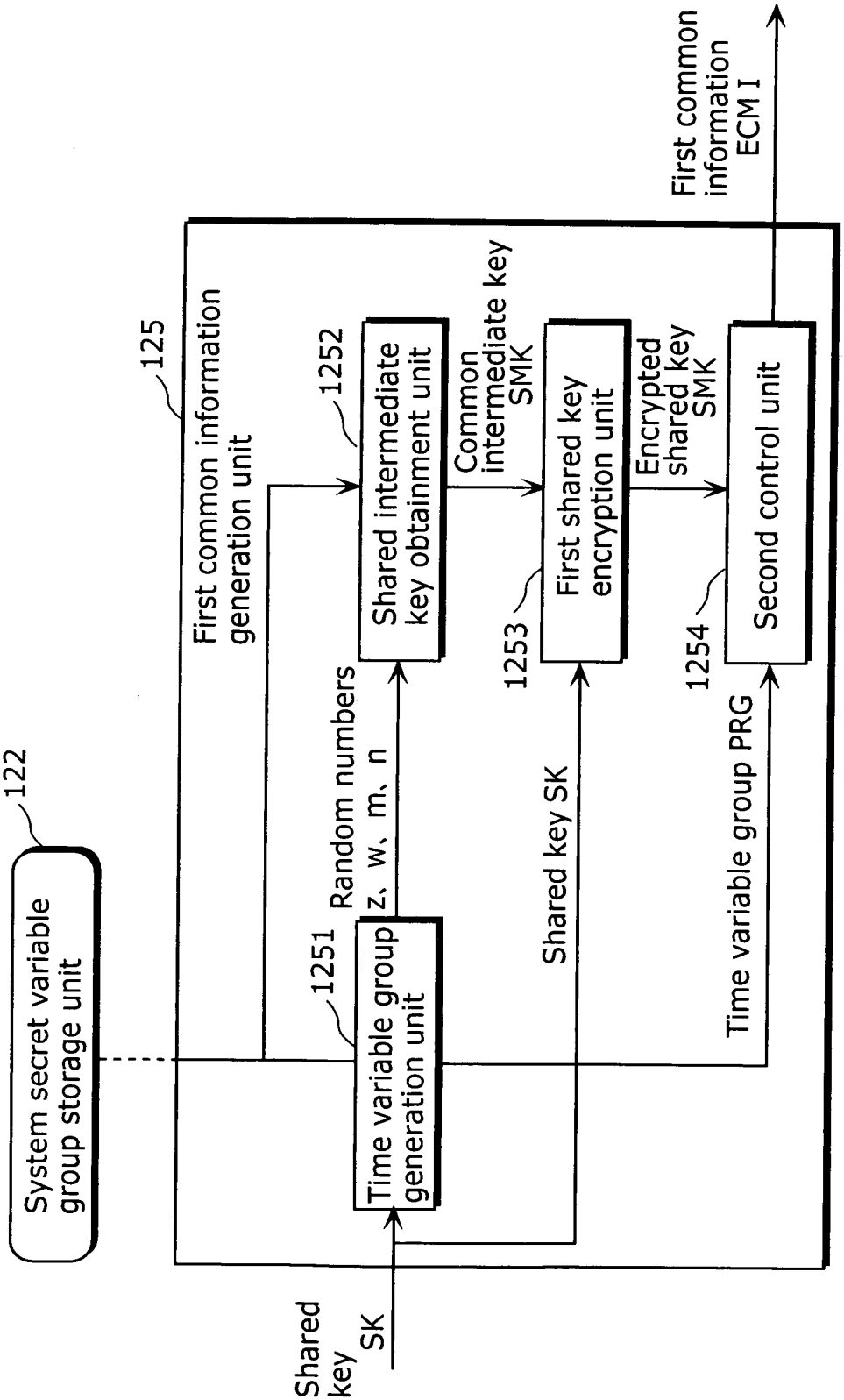

System secret variable group storage unit
122
125
First common information generation unit
Time variable group generation unit
1251
Random numbers z, w, m, n
Shared intermediate key obtainment unit
1252
Common intermediate key SMK
First shared key encryption unit
1253
Shared key SK
Encrypted shared key SMK
Second control unit
1254
Time variable group PRG
First common information ECM I
Shared key SK

FIG. 20

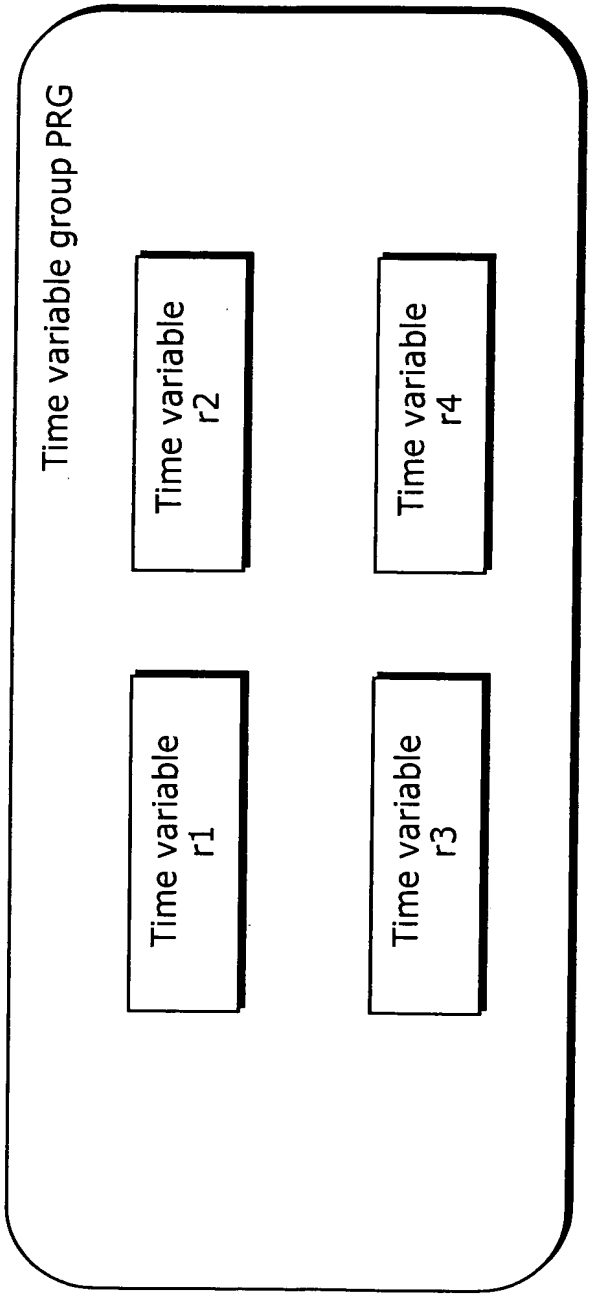

Time variable group PRG
Time variable r1
Time variable r2
Time variable r3
Time variable r4

FIG. 21

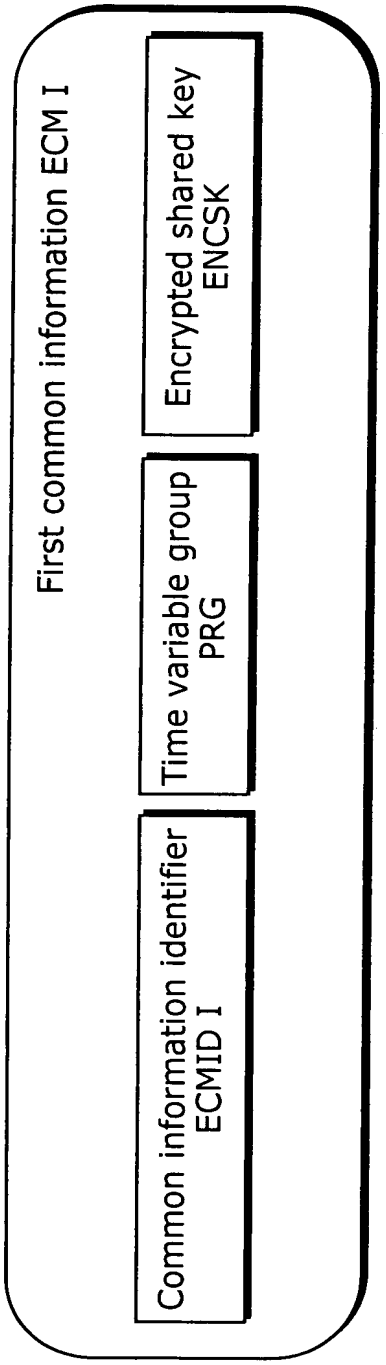

First common information ECM I
Common information identifier ECMID I
Time variable group PRG
Encrypted shared key ENCSK

FIG. 22

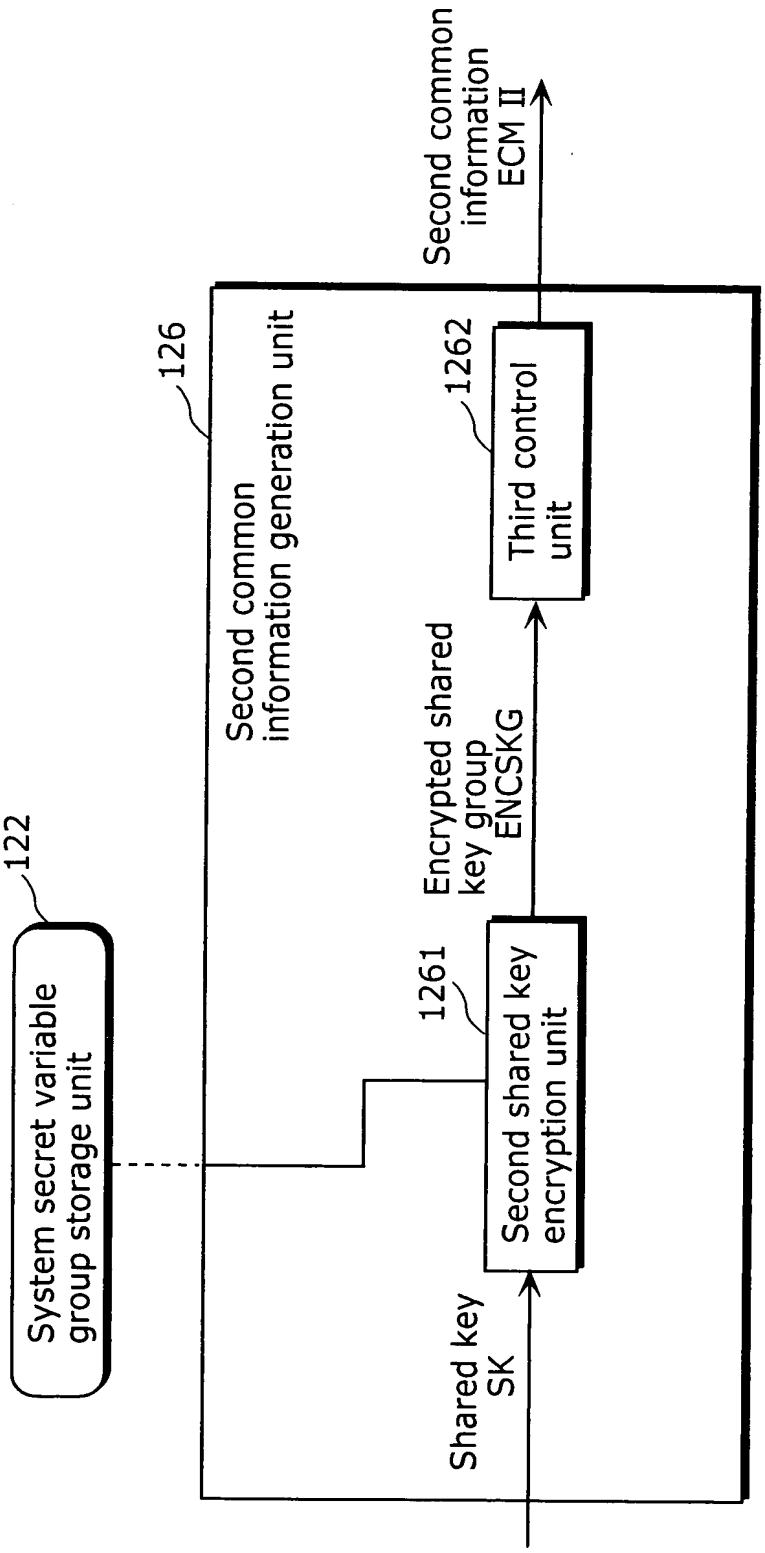

122
System secret variable group storage unit
126
Second common information generation unit
1261
Second shared key encryption unit
1262
Third control unit
Shared key SK
Encrypted shared key group ENCSKG
Second common information ECM II

FIG. 23

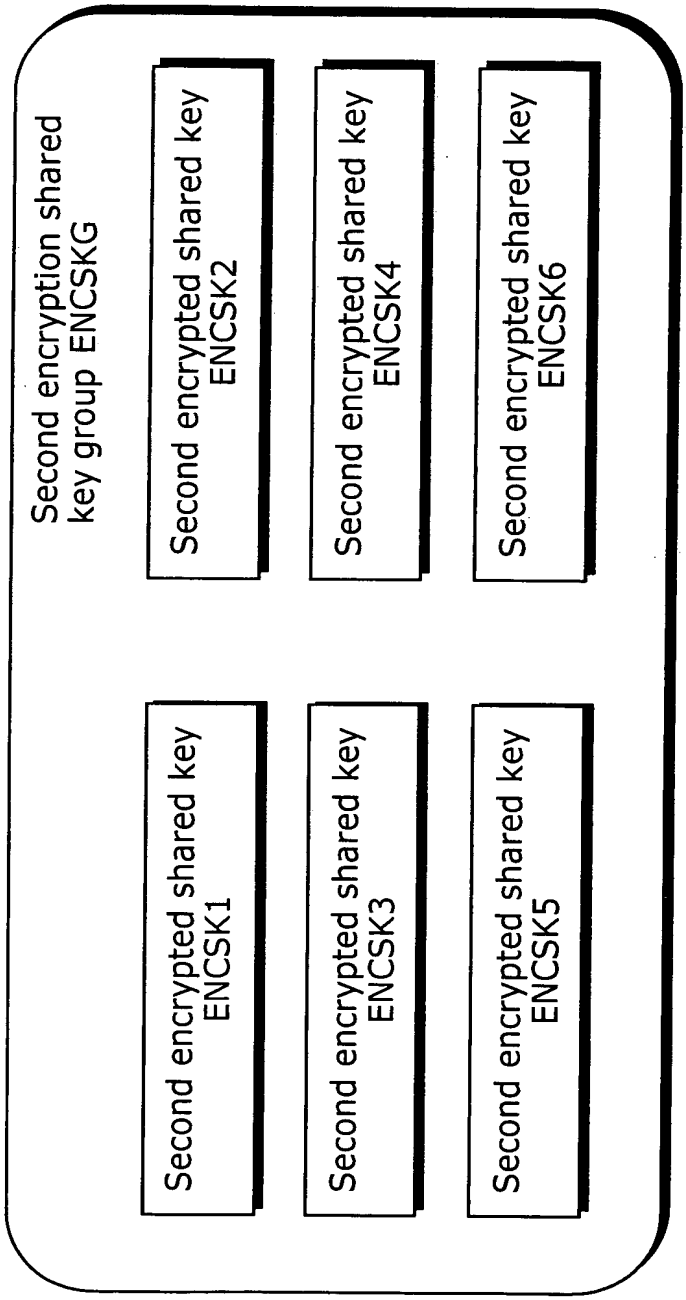

Second encryption shared key group ENCSKG
Second encrypted shared key ENCSK1
Second encrypted shared key ENCSK2
Second encrypted shared key ENCSK3
Second encrypted shared key ENCSK4
Second encrypted shared key ENCSK5
Second encrypted shared key ENCSK6

FIG. 24

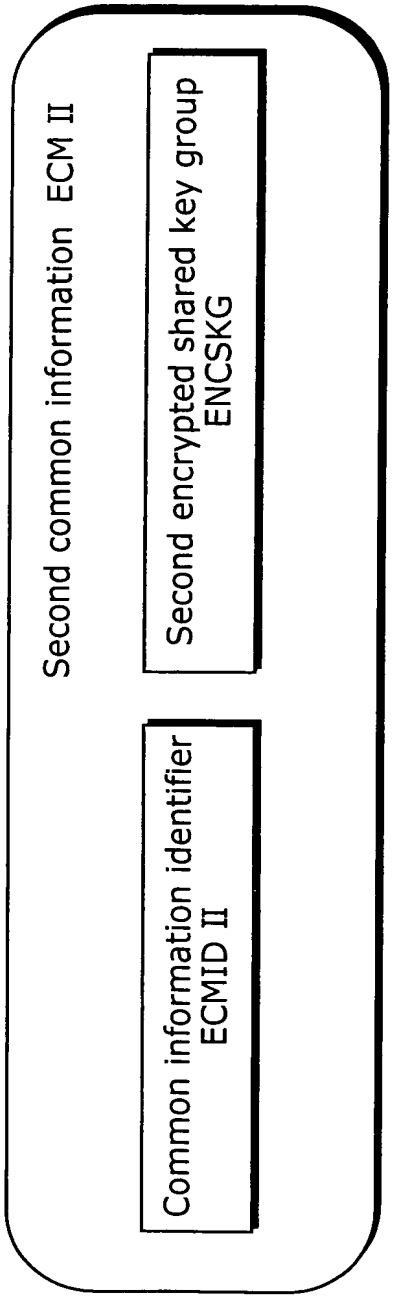

Second common information ECM II
Second encrypted shared key group ENCSKG
Common information identifier ECMID II

FIG. 25

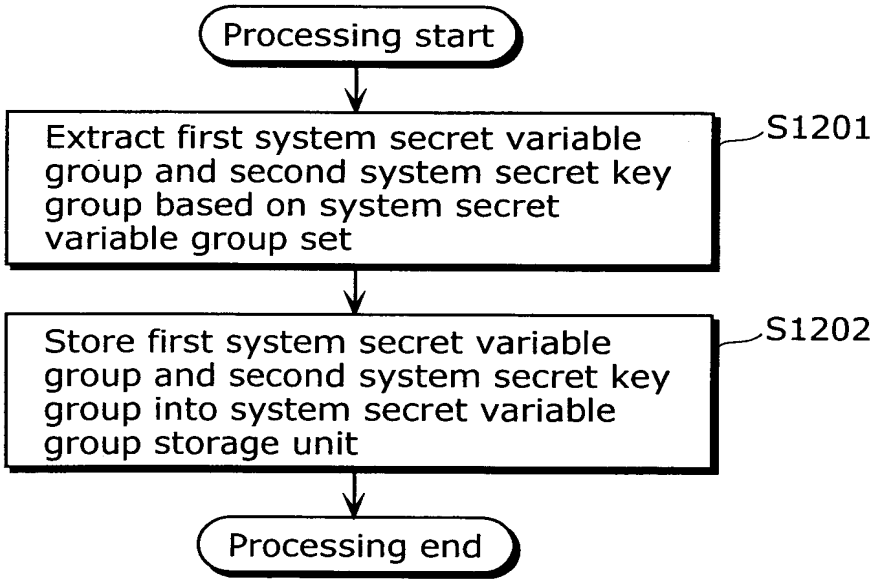

Processing start
Extract first system secret variable group and second system secret key group based on system secret variable group set
S1201
Store first system secret variable group and second system secret key group into system secret variable group storage unit
S1202
Processing end

FIG. 26

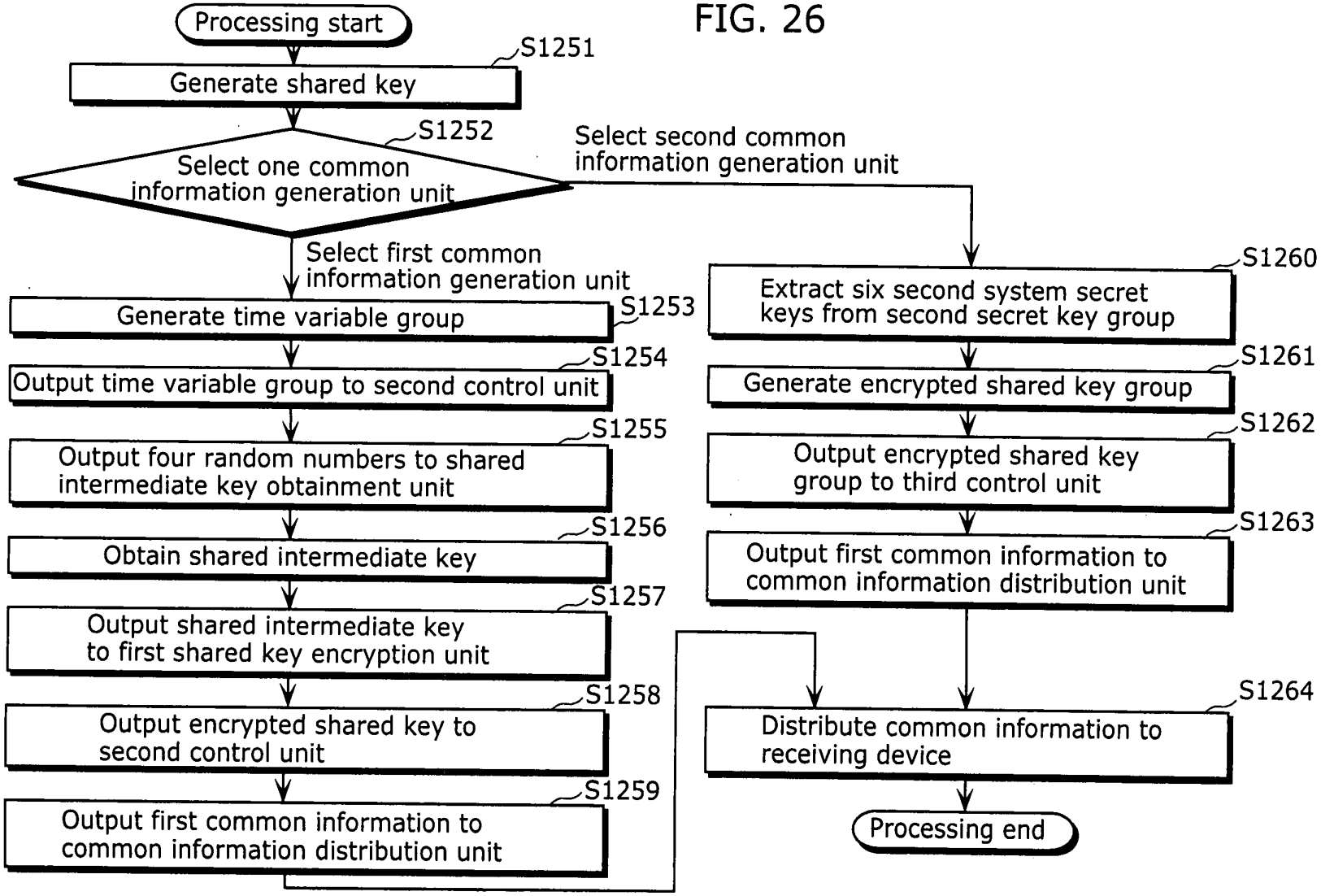

Processing start
S1251
Generate shared key
S1252
Select one common information generation unit
Select first common information generation unit
Select second common information generation unit
Generate time variable group
S1253
Output time variable group to second control unit
S1254
Output four random numbers to shared intermediate key obtainment unit
S1255
Obtain shared intermediate key
S1256
Output shared intermediate key to first shared key encryption unit
S1257
Output encrypted shared key to second control unit
S1258
Output first common information to common information distribution unit
S1259
Extract six second system secret keys from second secret key group
S1260
Generate encrypted shared key group
S1261
Output encrypted shared key group to third control unit
S1262
Output first common information to common information distribution unit
S1263
Distribute common information to receiving device
S1264
Processing end

FIG. 27

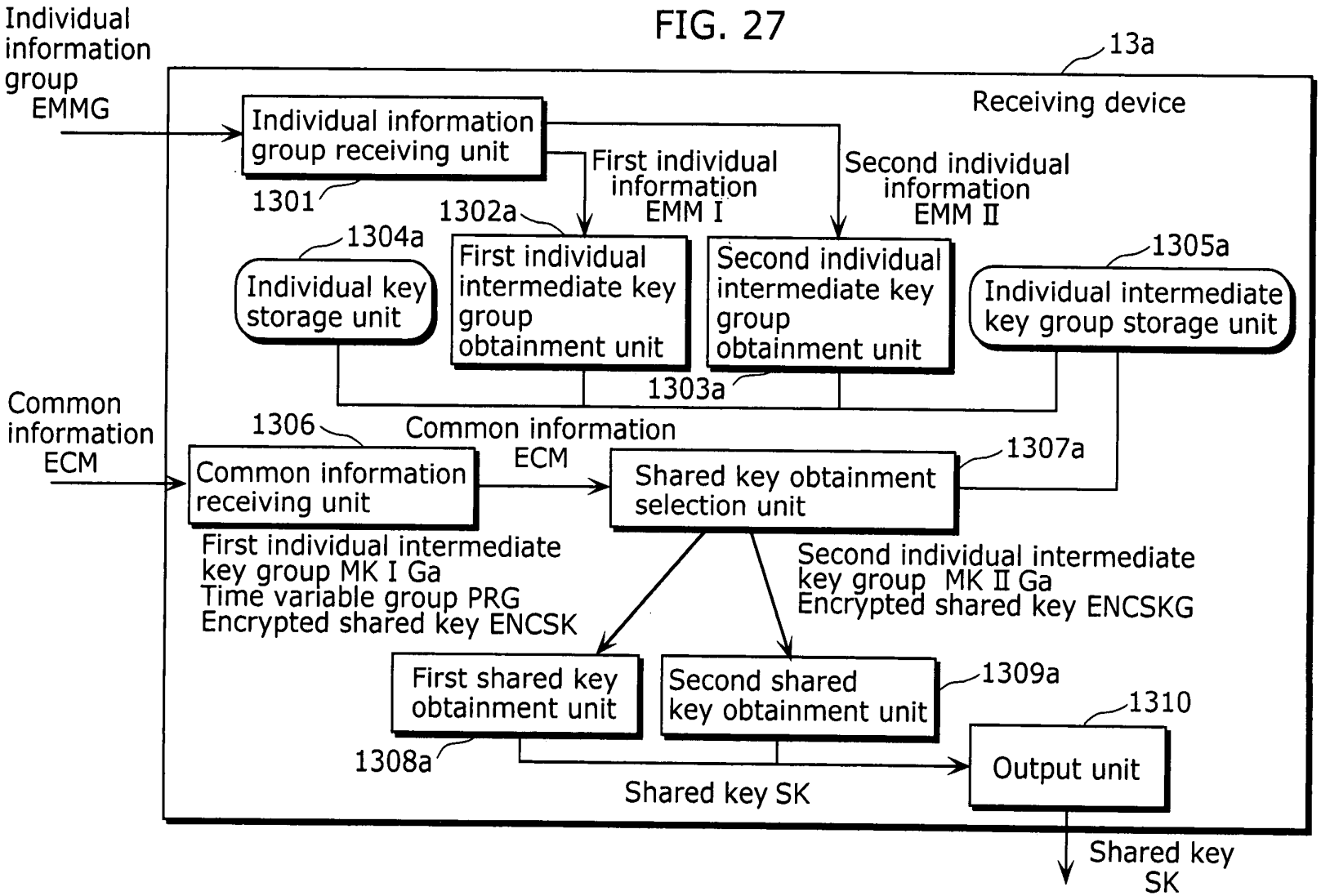

Individual information group EMMG
13a
Receiving device
Individual information group receiving unit
1301
First individual information EMM I
Second individual information EMM II
1302a
1304a
Individual key storage unit
First individual intermediate key group obtainment unit
Second individual intermediate key group obtainment unit
1305a
Individual intermediate key group storage unit
1303a
Common information ECM
1306
Common information receiving unit
Common information ECM
Shared key obtainment selection unit
1307a
First individual intermediate key group MK I Ga
Time variable group PRG
Encrypted shared key ENCSK
Second individual intermediate key group MK II Ga
Encrypted shared key ENCSKG
First shared key obtainment unit
Second shared key obtainment unit
1309a
1310
1308a
Output unit
Shared key SK
Shared key SK

FIG. 28

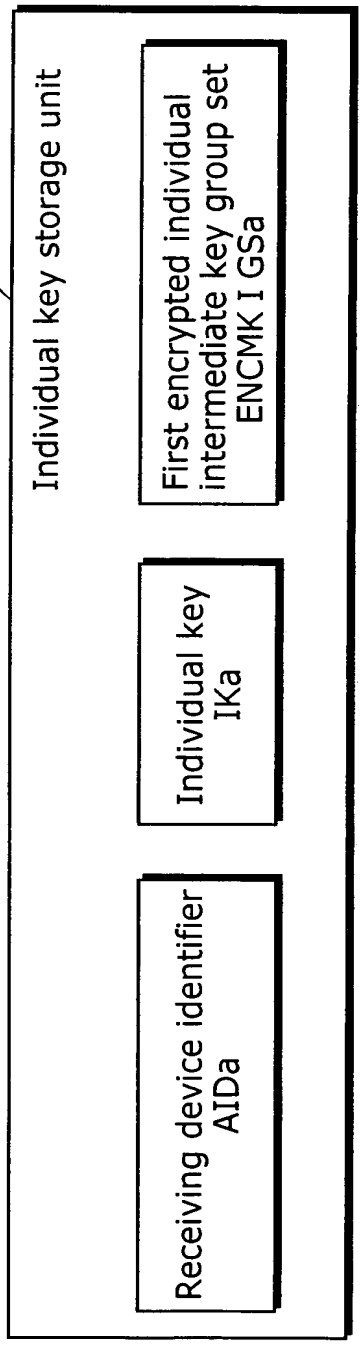

1304a
Individual key storage unit
Receiving device identifier AIDa
Individual key IKa
First encrypted individual intermediate key group set ENCMK I GSa

FIG. 29

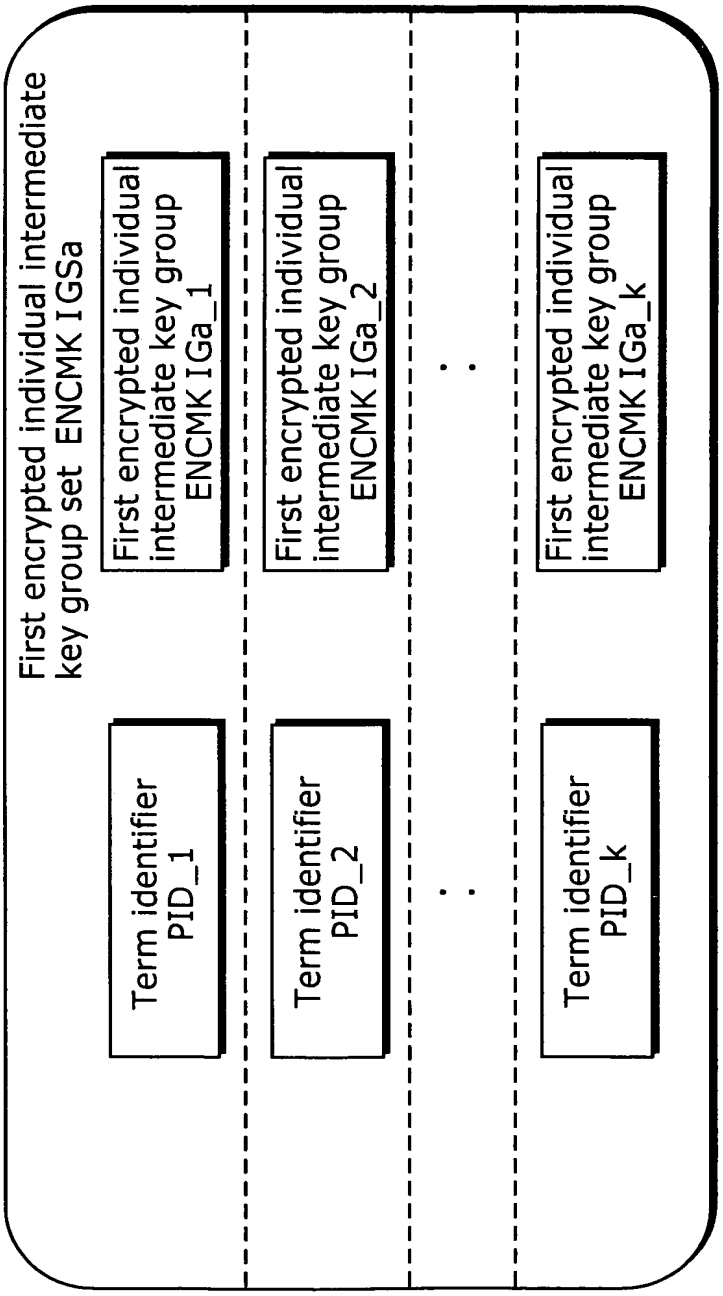

First encrypted individual intermediate key group set ENCMK IGSa
Term identifier PID_1
First encrypted individual intermediate key group ENCMK IGa_1
Term identifier PID_2
First encrypted individual intermediate key group ENCMK IGa_2
Term identifier PID_k
First encrypted individual intermediate key group ENCMK IGa_k

FIG. 30

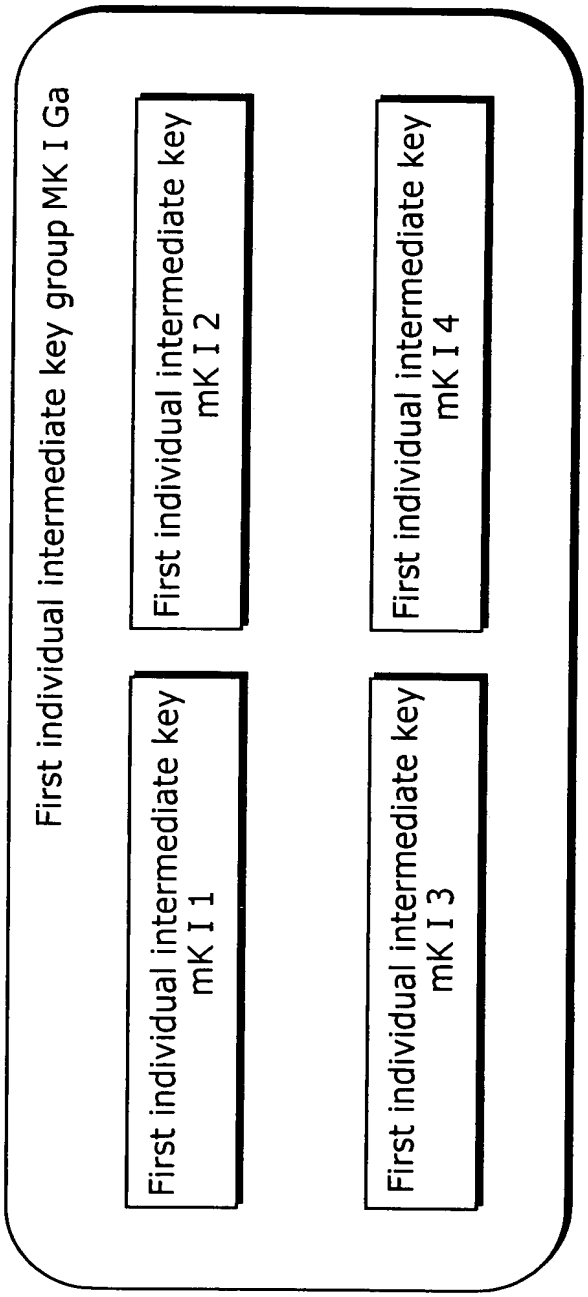

First individual intermediate key group MK I Ga
First individual intermediate key mK I 1
First individual intermediate key mK I 2
First individual intermediate key mK I 3
First individual intermediate key mK I 4

FIG. 31

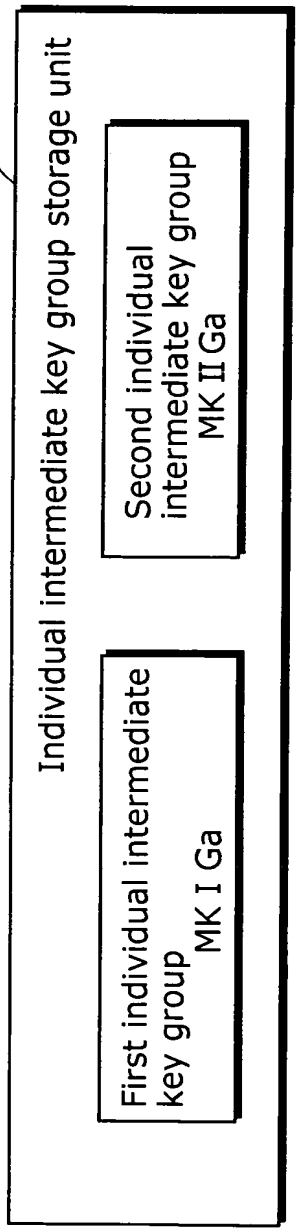

1305a
Individual intermediate key group storage unit
First individual intermediate key group MK I Ga
Second individual intermediate key group MK II Ga

FIG. 32

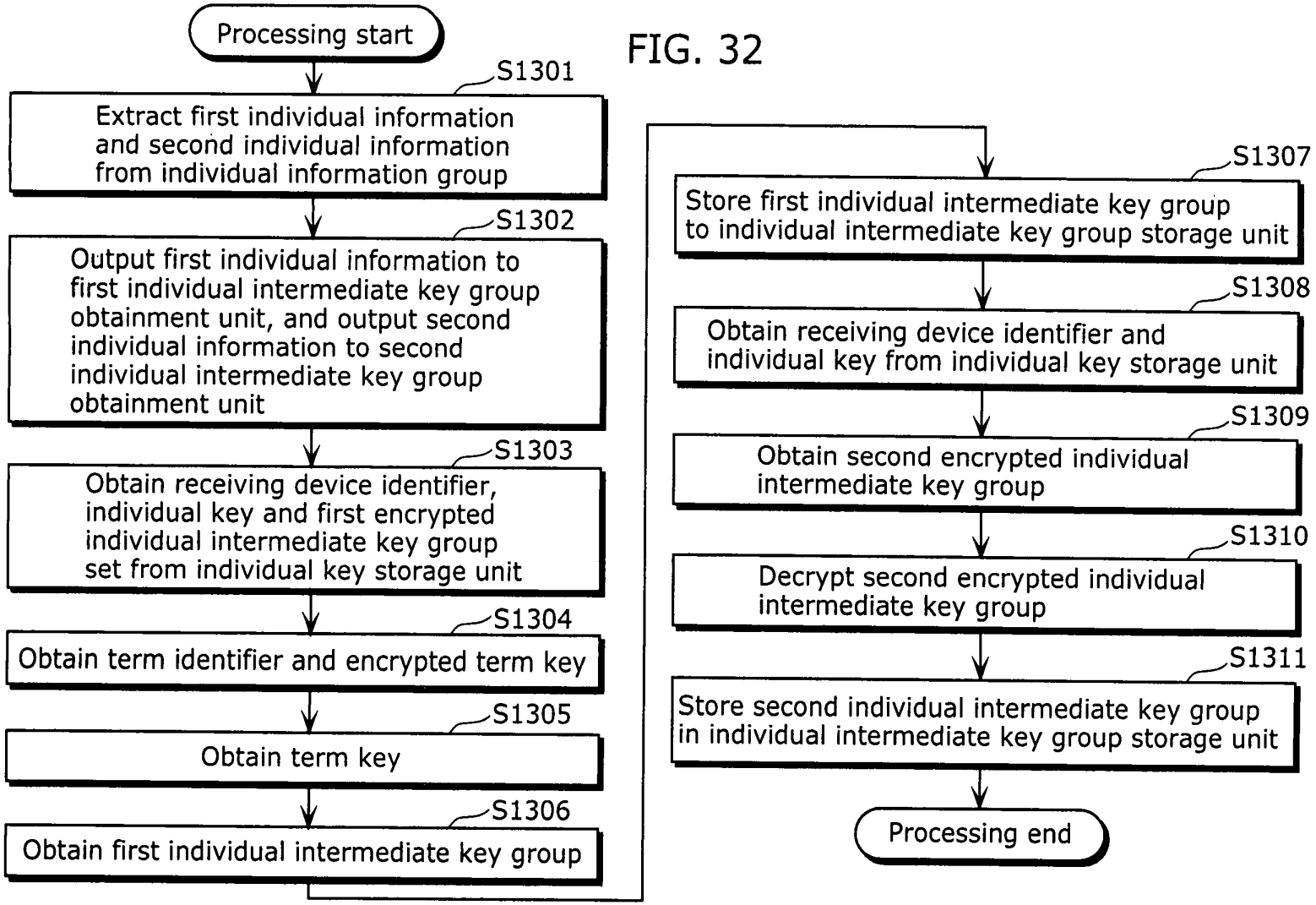

Processing start
S1301
Extract first individual information and second individual information from individual information group
S1302
Output first individual information to first individual intermediate key group obtainment unit, and output second individual information to second individual intermediate key group obtainment unit
S1303
Obtain receiving device identifier, individual key and first encrypted individual intermediate key group set from individual key storage unit
S1304
Obtain term identifier and encrypted term key
S1305
Obtain term key
S1306
Obtain first individual intermediate key group
S1307
Store first individual intermediate key group to individual intermediate key group storage unit
S1308
Obtain receiving device identifier and individual key from individual key storage unit
S1309
Obtain second encrypted individual intermediate key group
S1310
Decrypt second encrypted individual intermediate key group
S1311
Store second individual intermediate key group in individual intermediate key group storage unit
Processing end

FIG. 33

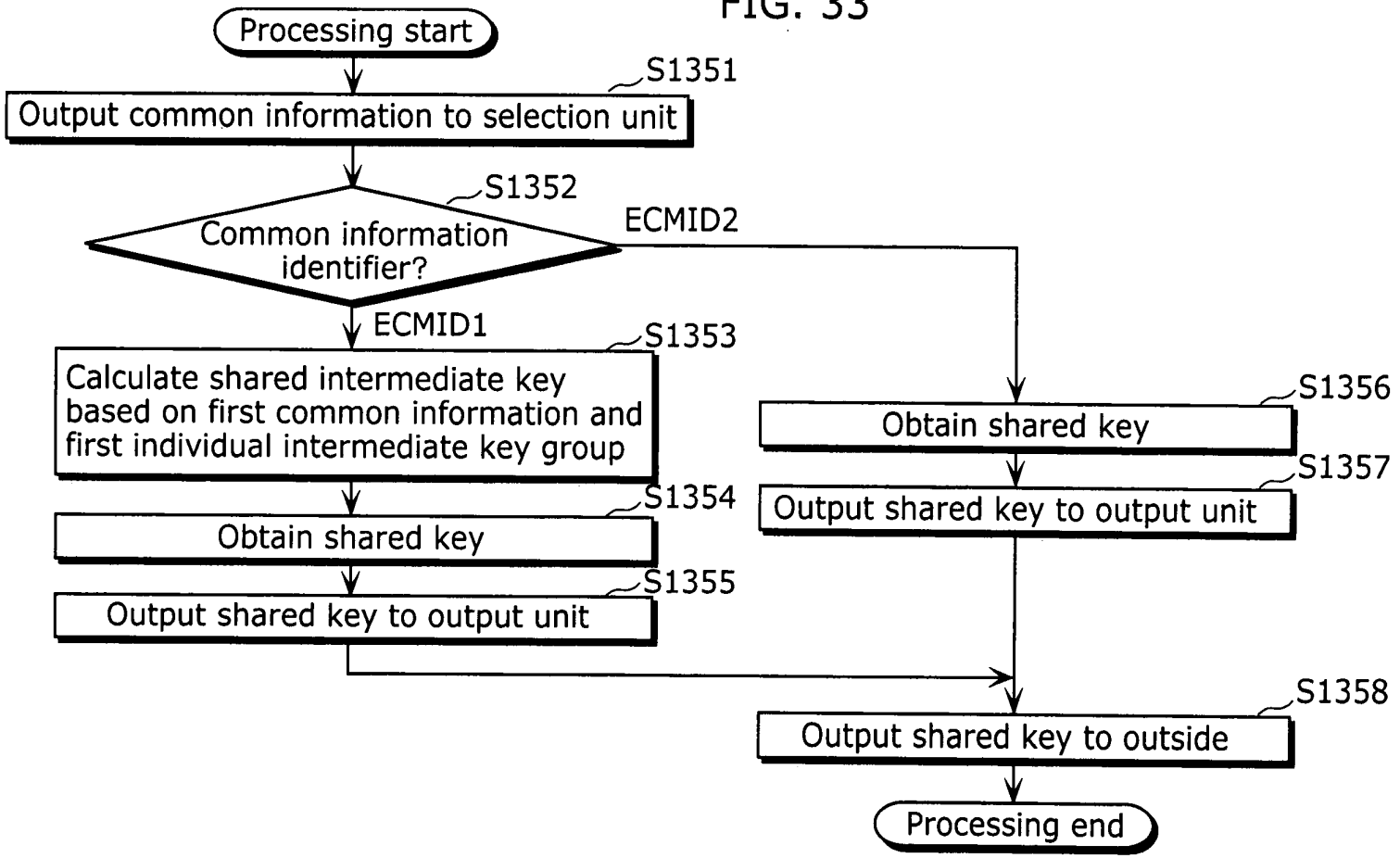

Processing start
S1351
Output common information to selection unit
S1352
Common information identifier?
ECMID2
ECMID1
S1353
Calculate shared intermediate key based on first common information and first individual intermediate key group
S1354
Obtain shared key
S1355
Output shared key to output unit
S1356
Obtain shared key
S1357
Output shared key to output unit
S1358
Output shared key to outside
Processing end

FIG. 34

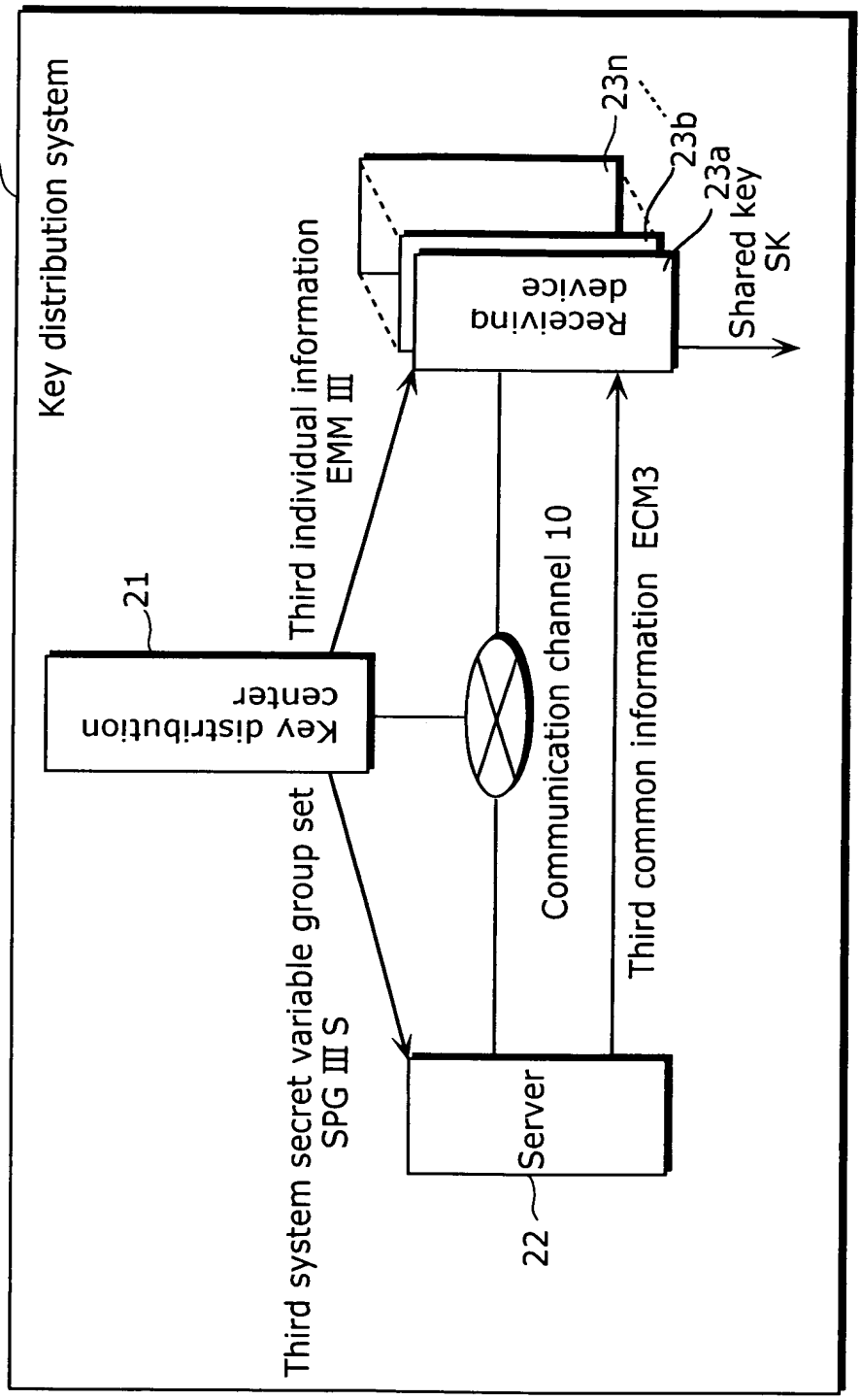

2
Key distribution system
21
Key distribution center
Third individual information EMM III
23n
23b
23a
Receiving device
Shared key SK
Communication channel 10
Third common information ECM3
Third system secret variable group set SPG III S
Server
22

FIG. 35

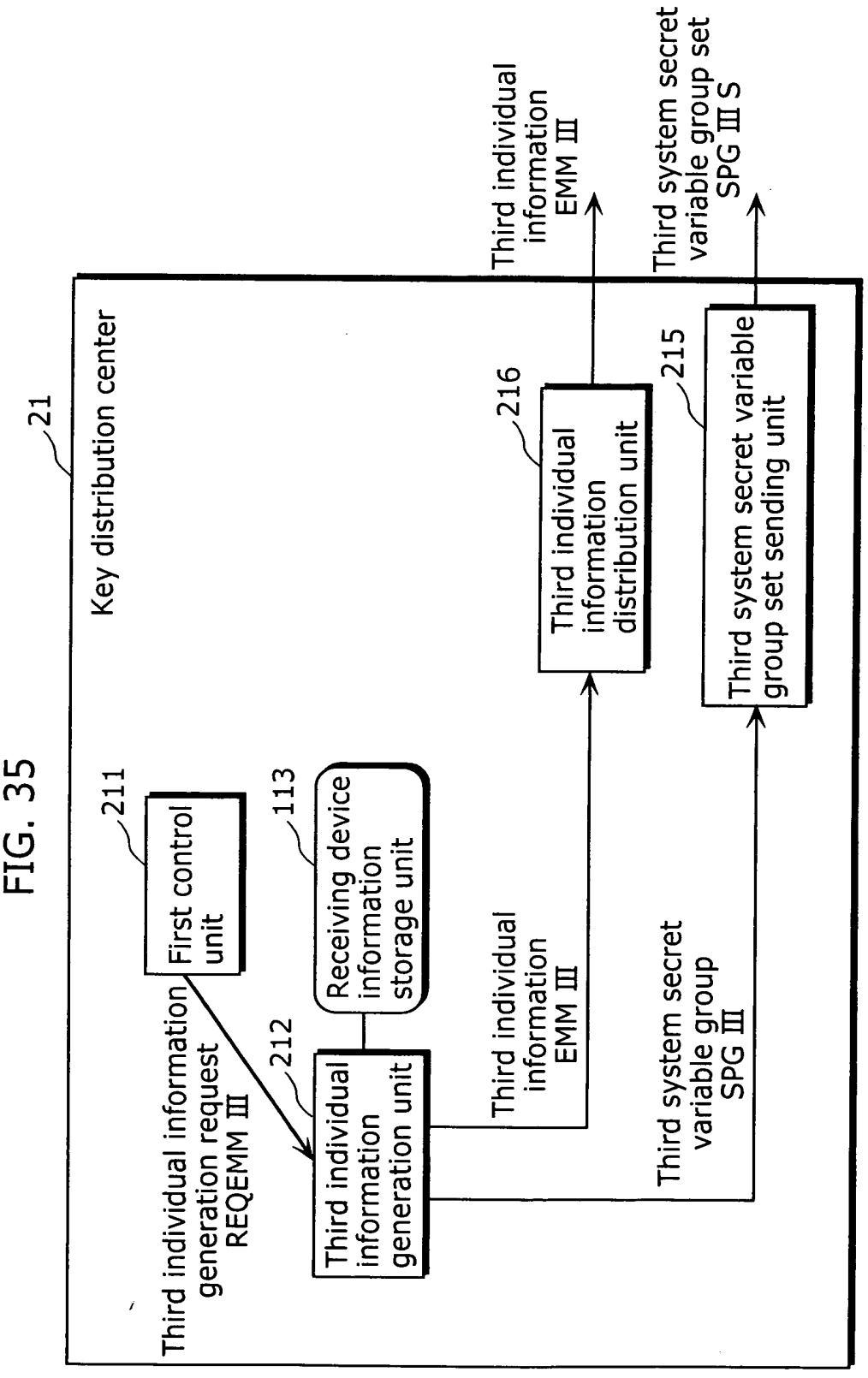

21
Key distribution center
211
First control unit
113
Receiving device information storage unit
212
Third individual information generation unit
216
Third individual information distribution unit
215
Third system secret variable group set sending unit
Third individual information generation request REQEMM III
Third individual information EMM III
Third system secret variable group SPG III
Third individual information EMM III
Third system secret variable group set SPG III S

FIG. 36

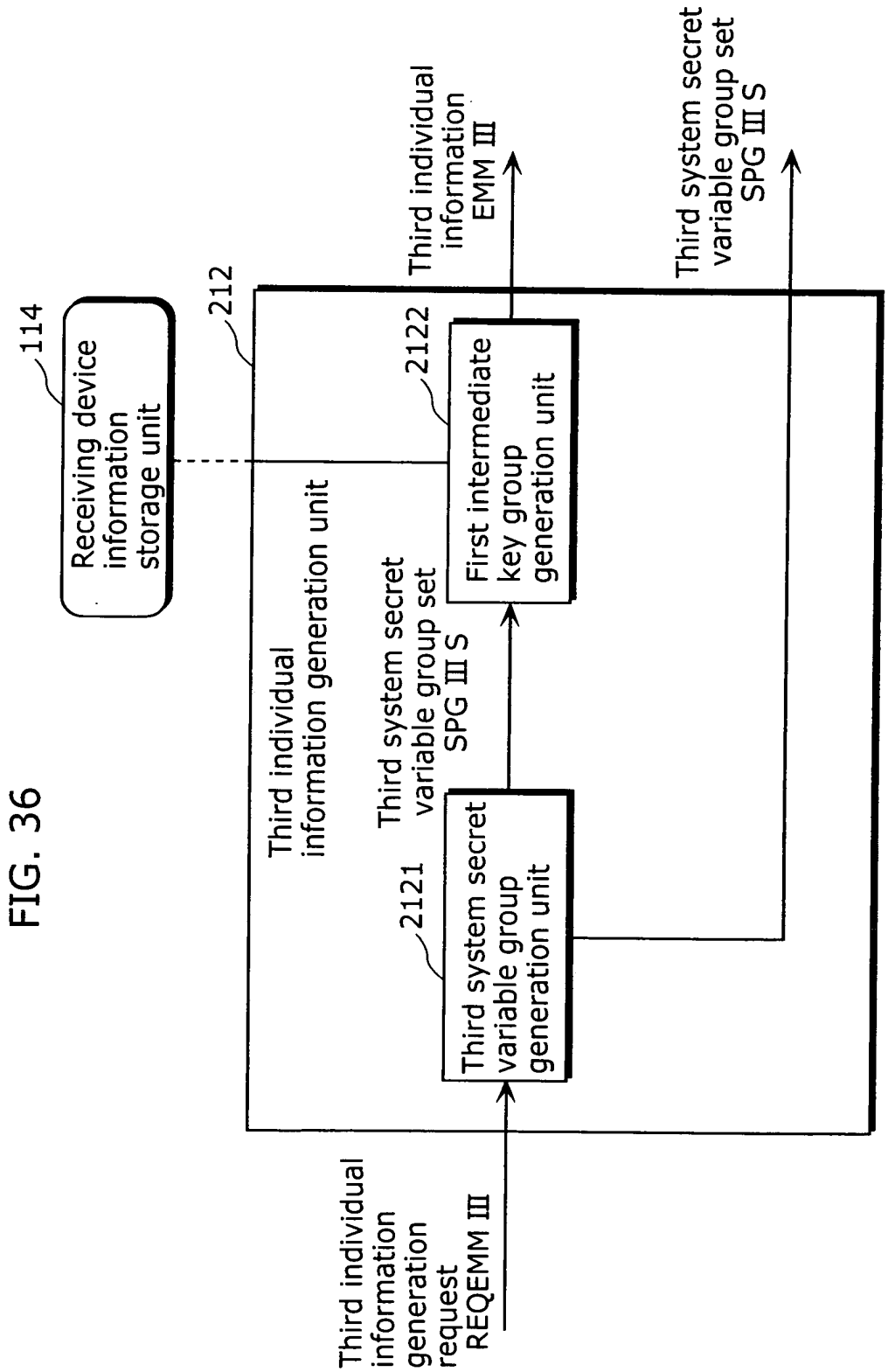

Third individual information REQEMM III
Third individual information generation request
Receiving device information storage unit
114
212
Third individual information generation unit
2121
Third system secret variable group generation unit
Third system secret variable group set SPG III S
2122
First intermediate key group generation unit
Third individual information EMM III
Third system secret variable group set SPG III S

FIG. 37

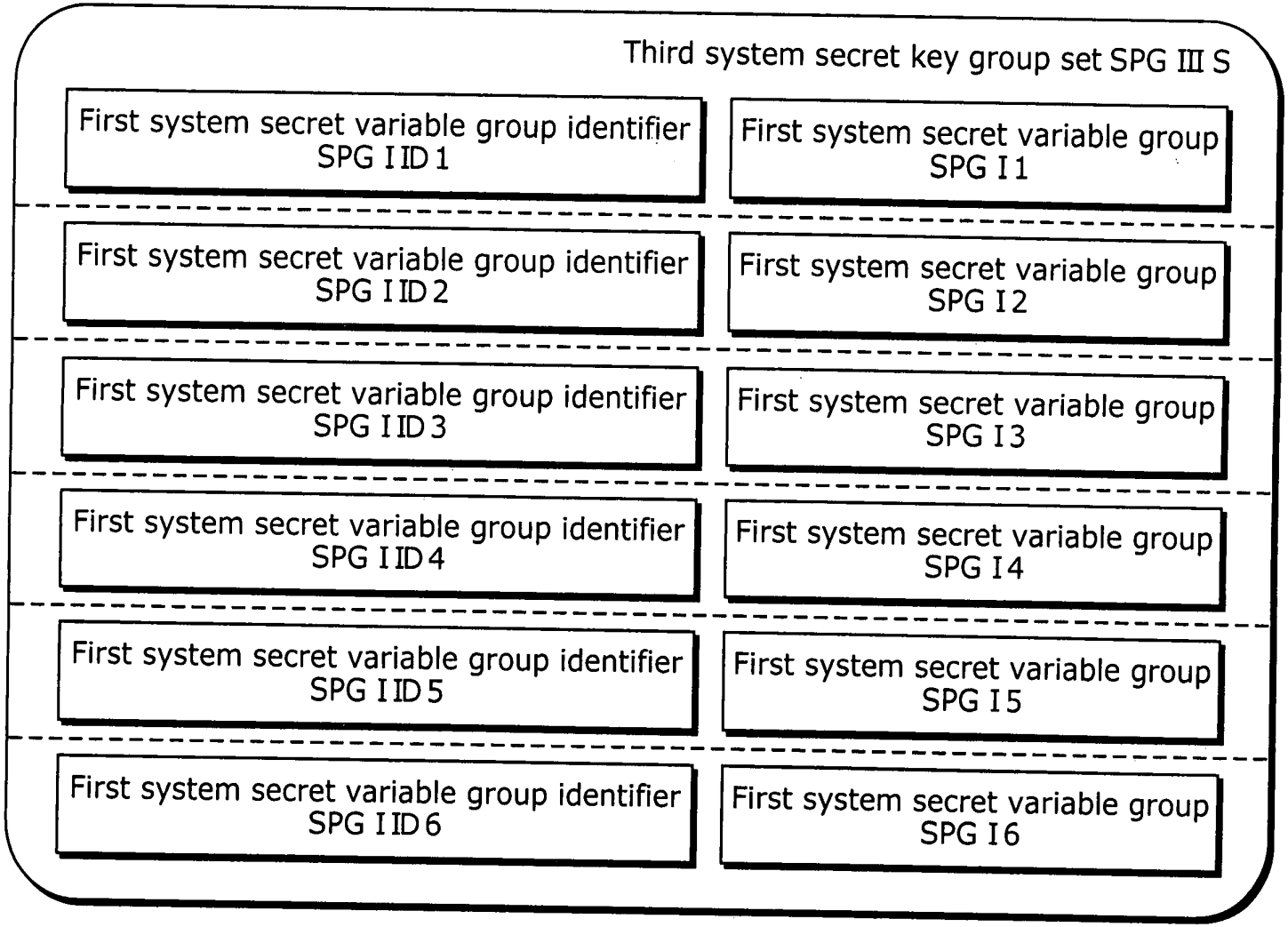

Third system secret key group set SPG III S
First system secret variable group identifier SPG I ID 1
First system secret variable group SPG I 1
First system secret variable group identifier SPG I ID 2
First system secret variable group SPG I 2
First system secret variable group identifier SPG I ID 3
First system secret variable group SPG I 3
First system secret variable group identifier SPG I ID 4
First system secret variable group SPG I 4
First system secret variable group identifier SPG I ID 5
First system secret variable group SPG I 5
First system secret variable group identifier SPG I ID 6
First system secret variable group SPG I 6

FIG. 38

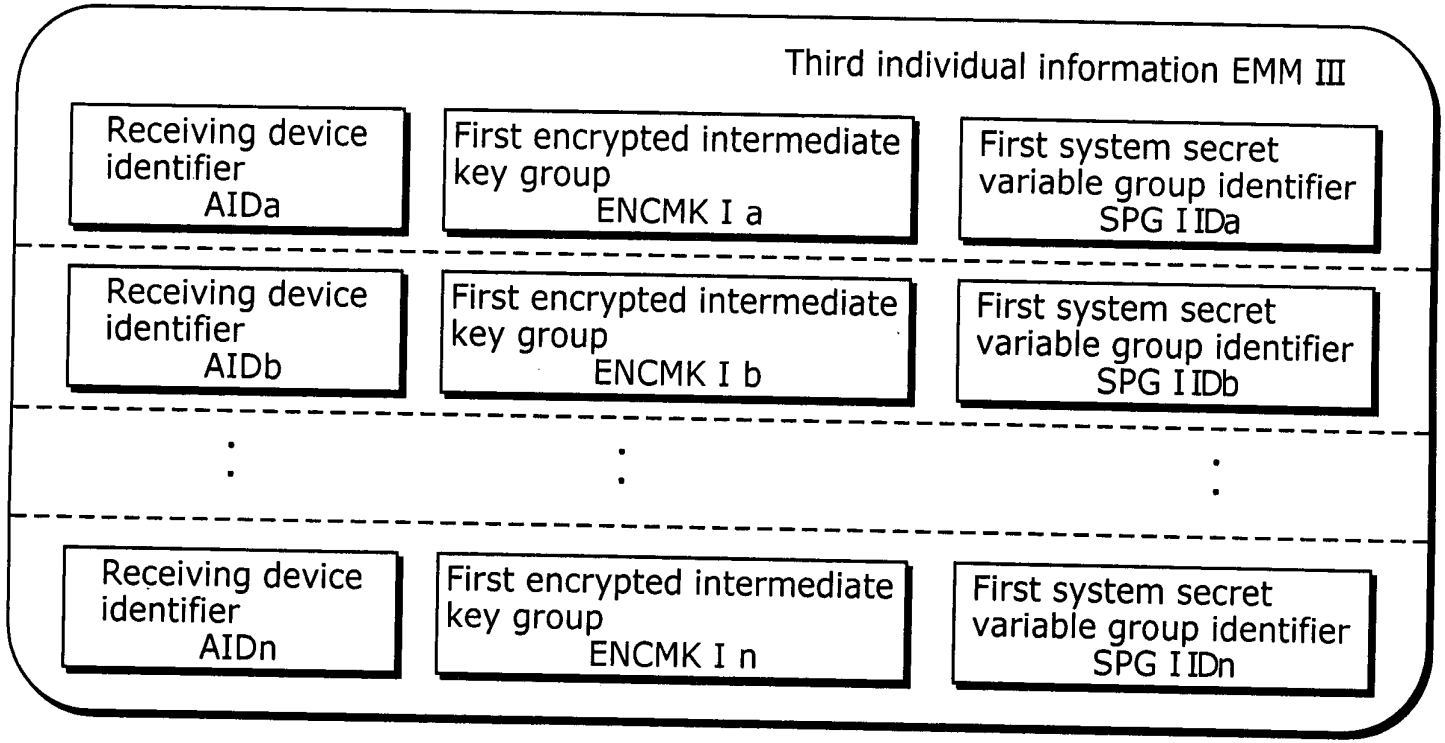

Third individual information EMM III
Receiving device identifier AIDa
First encrypted intermediate key group ENCMK I a
First system secret variable group identifier SPG I IDa
Receiving device identifier AIDb
First encrypted intermediate key group ENCMK I b
First system secret variable group identifier SPG I IDb
Receiving device identifier AIDn
First encrypted intermediate key group ENCMK I n
First system secret variable group identifier SPG I IDn

FIG. 39

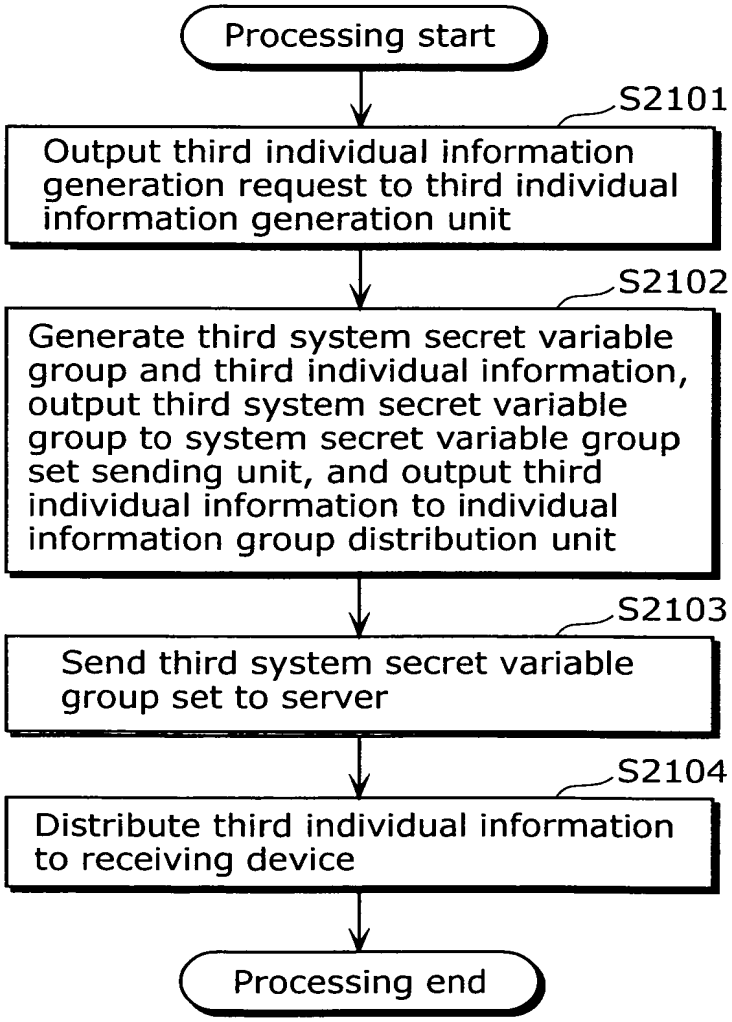

Processing start
S2101
Output third individual information generation request to third individual information generation unit
S2102
Generate third system secret variable group and third individual information, output third system secret variable group to system secret variable group set sending unit, and output third individual information to individual information group distribution unit
S2103
Send third system secret variable group set to server
S2104
Distribute third individual information to receiving device
Processing end

FIG. 40

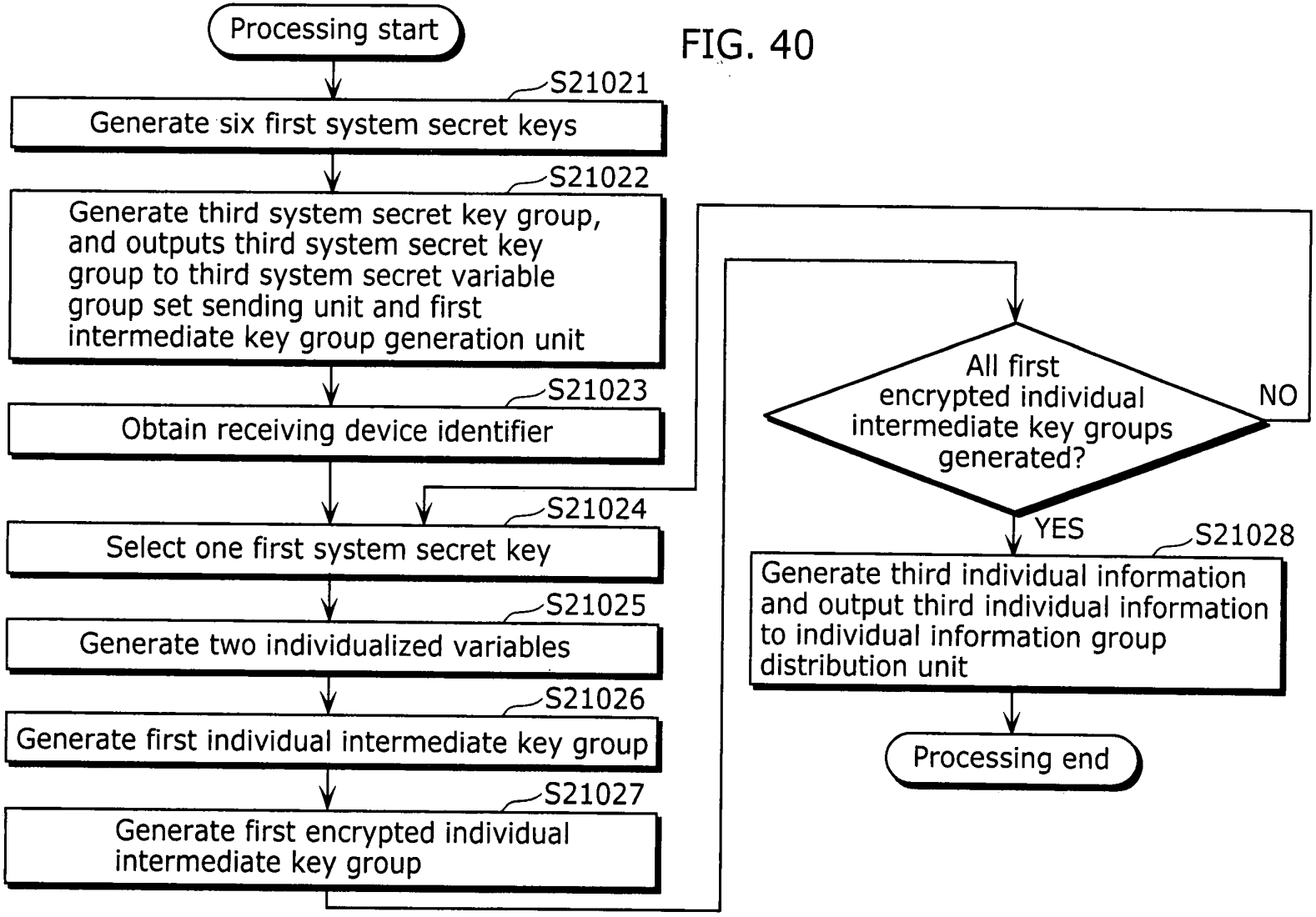

Processing start
S21021
Generate six first system secret keys
S21022
Generate third system secret key group, and outputs third system secret key group to third system secret variable group set sending unit and first intermediate key group generation unit
S21023
Obtain receiving device identifier
S21024
Select one first system secret key
S21025
Generate two individualized variables
S21026
Generate first individual intermediate key group
S21027
Generate first encrypted individual intermediate key group
All first encrypted individual intermediate key groups generated?
NO
YES
S21028
Generate third individual information and output third individual information to individual information group distribution unit
Processing end

FIG. 41

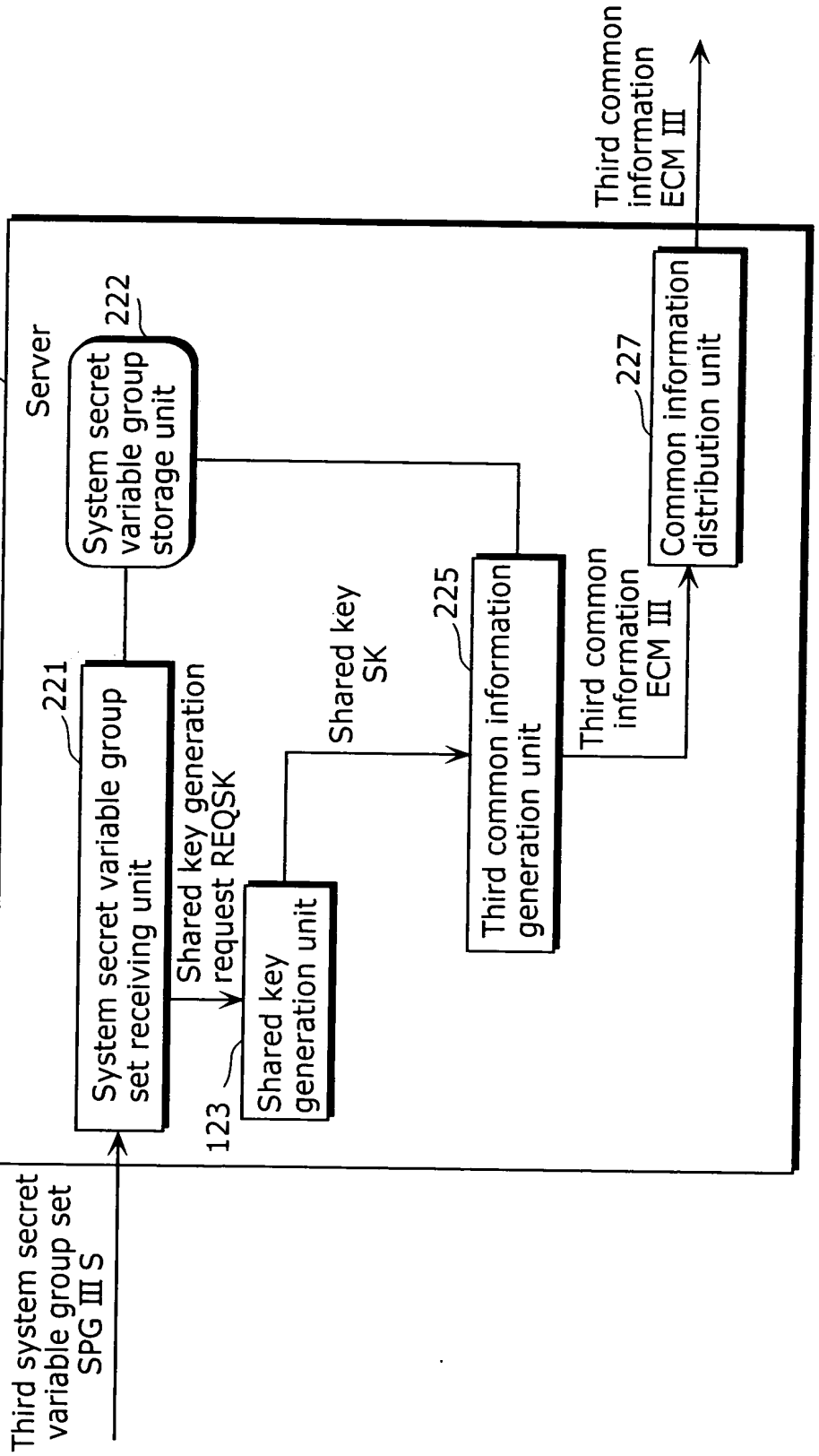

22
Server
222
System secret variable group storage unit
221
System secret variable group set receiving unit
Shared key generation request REQSK
123
Shared key generation unit
Shared key SK
225
Third common information generation unit
Third common information ECM III
227
Common information distribution unit
Third common information ECM III
Third system secret variable group set SPG III S

FIG. 42

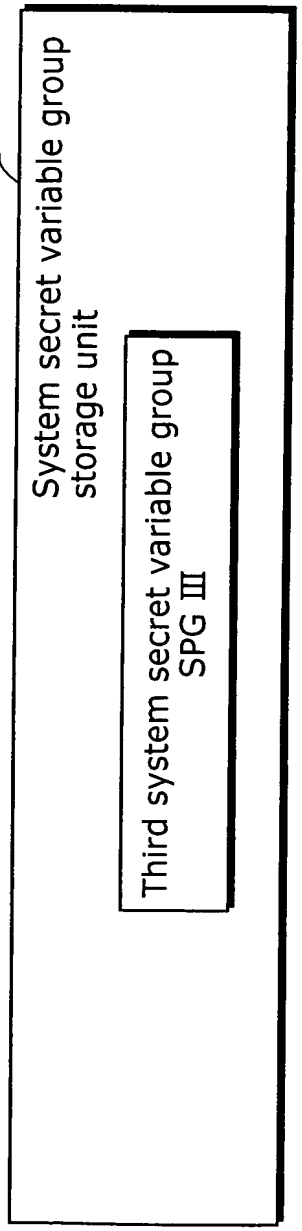

222
System secret variable group storage unit
Third system secret variable group SPG III

FIG. 43

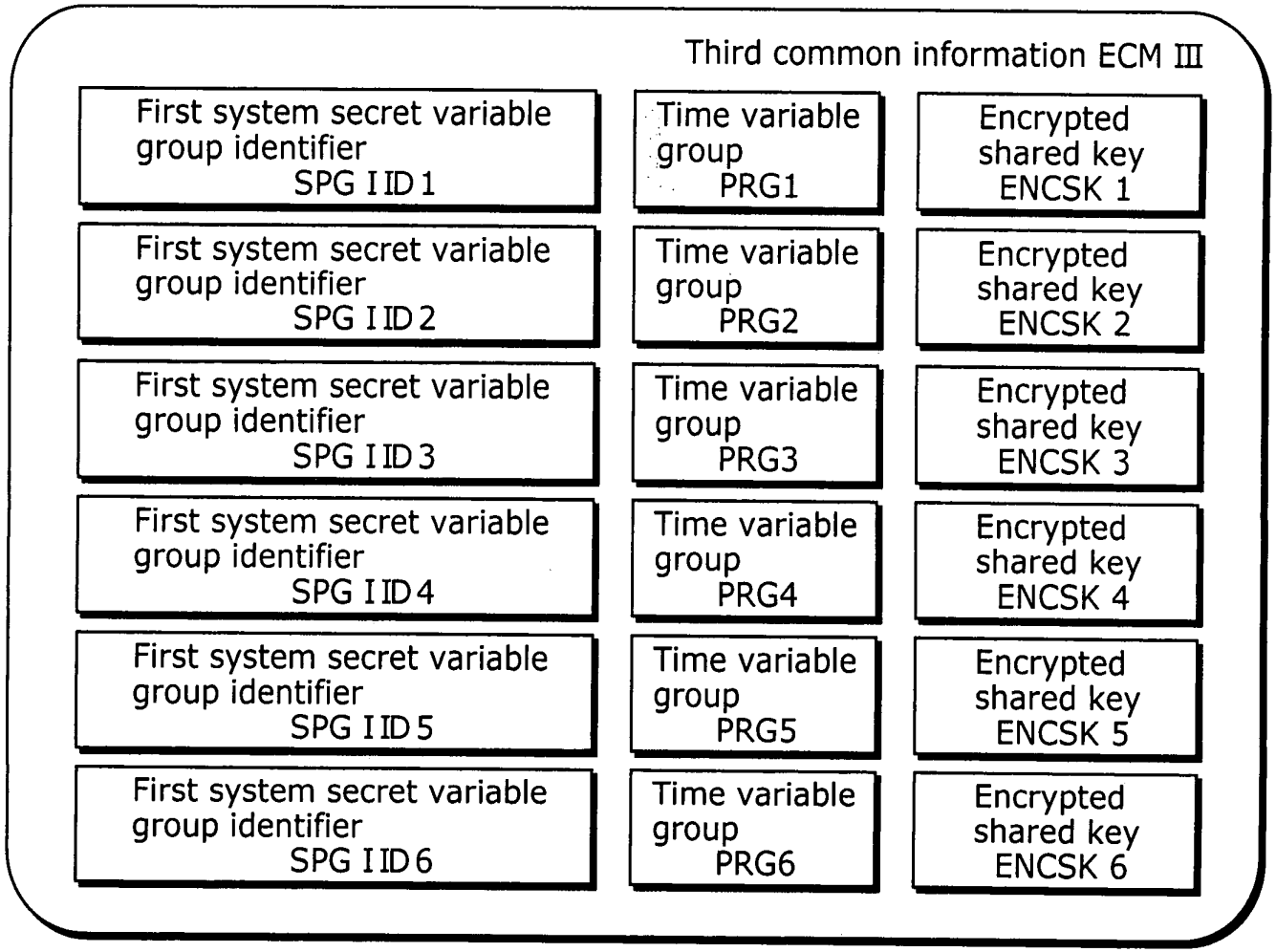

Third common information ECM III
First system secret variable group identifier SPG I ID 1
Time variable group PRG1
Encrypted shared key ENCSK 1
First system secret variable group identifier SPG I ID 2
Time variable group PRG2
Encrypted shared key ENCSK 2
First system secret variable group identifier SPG I ID 3
Time variable group PRG3
Encrypted shared key ENCSK 3
First system secret variable group identifier SPG I ID 4
Time variable group PRG4
Encrypted shared key ENCSK 4
First system secret variable group identifier SPG I ID 5
Time variable group PRG5
Encrypted shared key ENCSK 5
First system secret variable group identifier SPG I ID 6
Time variable group PRG6
Encrypted shared key ENCSK 6

FIG. 44

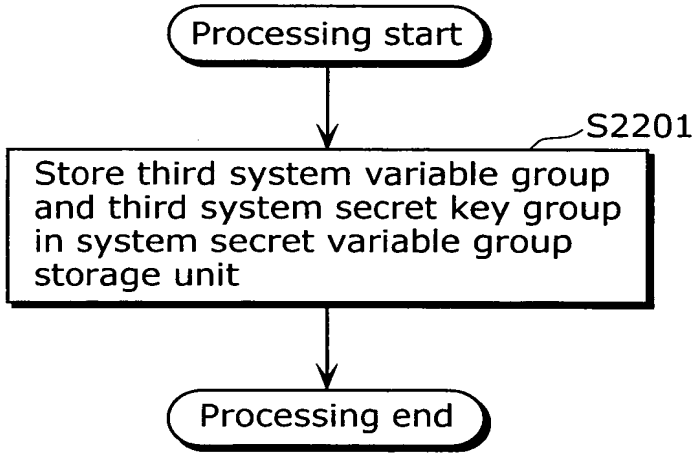

Processing start
S2201
Store third system variable group and third system secret key group in system secret variable group storage unit
Processing end

FIG. 45

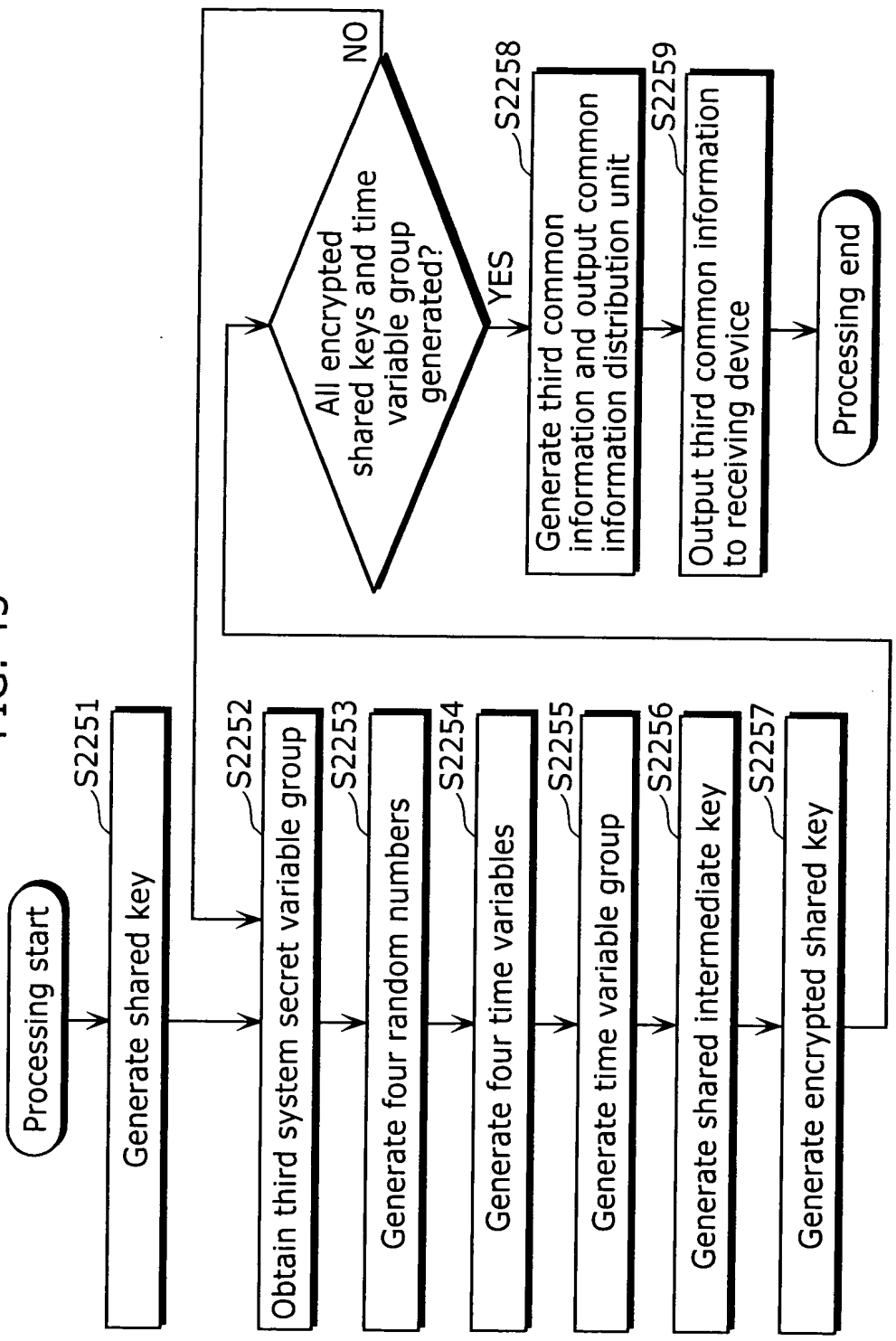

Processing start
S2251
Generate shared key
S2252
Obtain third system secret variable group
S2253
Generate four random numbers
S2254
Generate four time variables
S2255
Generate time variable group
S2256
Generate shared intermediate key
S2257
Generate encrypted shared key
All encrypted shared keys and time variable group generated?
NO
YES
S2258
Generate third common information and output common information distribution unit
S2259
Output third common information to receiving device
Processing end

FIG. 46

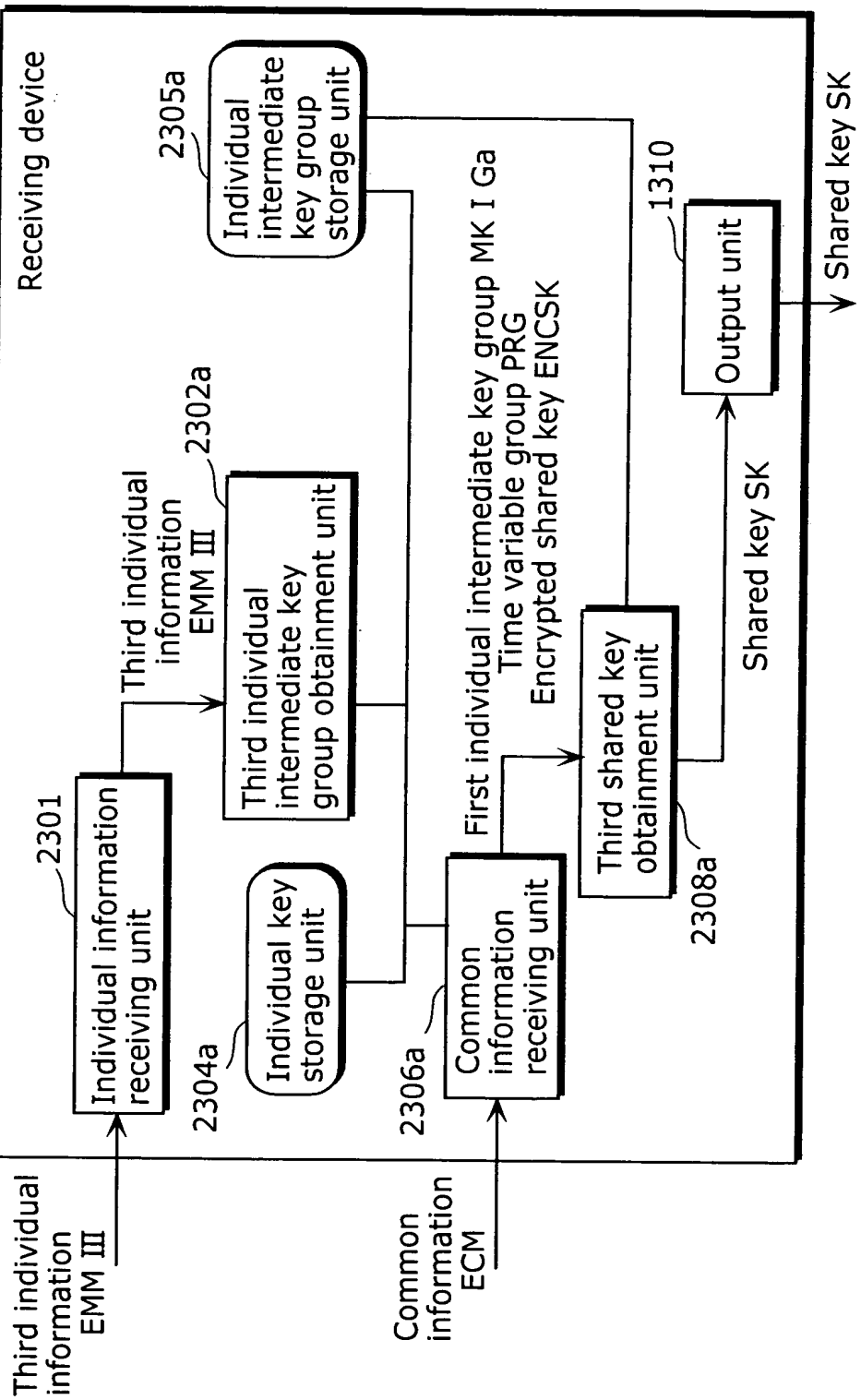

23a
Receiving device
2305a
Individual intermediate key group storage unit
1310
Output unit
Shared key SK
Shared key SK
2302a
Third individual information EMM III
Third individual intermediate key group obtainment unit
2301
Individual information receiving unit
2304a
Individual key storage unit
2306a
Common information receiving unit
First individual intermediate key group MK I Ga
Time variable group PRG
Encrypted shared key ENCSK
Third shared key obtainment unit
2308a
Third individual information EMM III
Common information ECM

FIG. 47

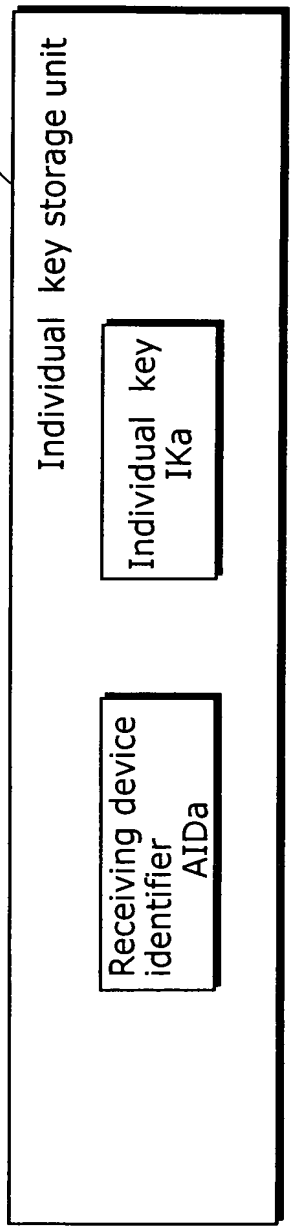

2304a
Individual key storage unit
Individual key IKa
Receiving device identifier AIDa

FIG. 48

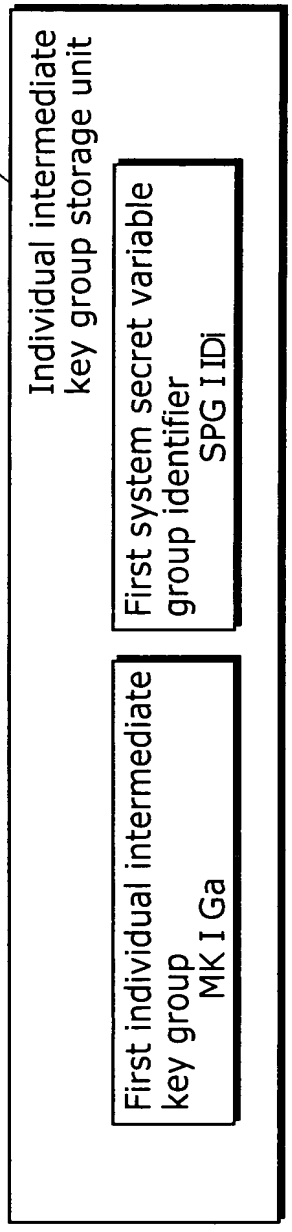

2305a
Individual intermediate key group storage unit
First system secret variable group identifier SPG I IDi
First individual intermediate key group MK I Ga

FIG. 49

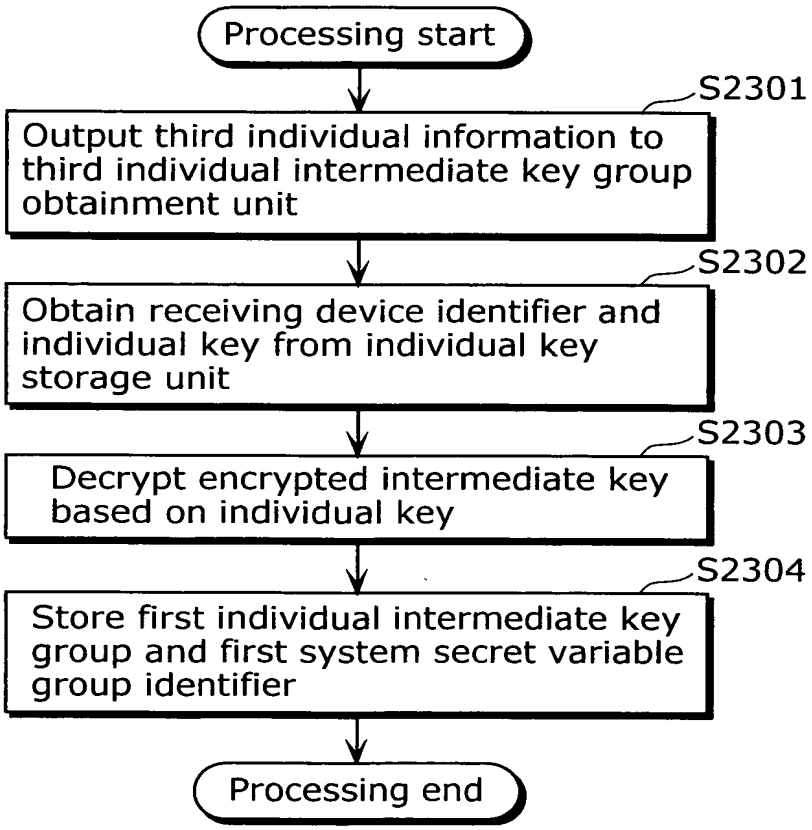

Processing start
S2301
Output third individual information to third individual intermediate key group obtainment unit
S2302
Obtain receiving device identifier and individual key from individual key storage unit
S2303
Decrypt encrypted intermediate key based on individual key
S2304
Store first individual intermediate key group and first system secret variable group identifier
Processing end

FIG. 50

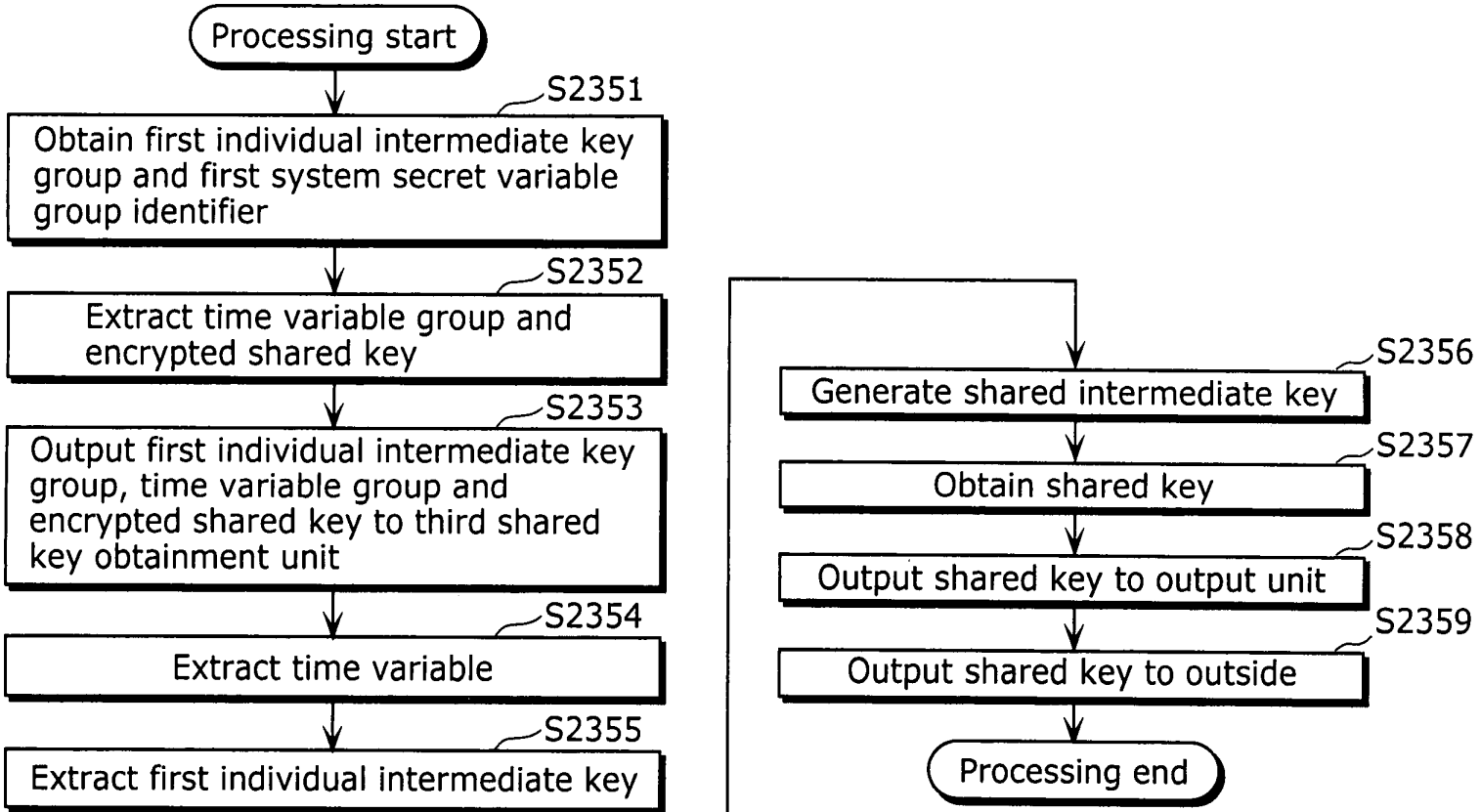

Processing start
S2351
Obtain first individual intermediate key group and first system secret variable group identifier
S2352
Extract time variable group and encrypted shared key
S2353
Output first individual intermediate key group, time variable group and encrypted shared key to third shared key obtainment unit
S2354
Extract time variable
S2355
Extract first individual intermediate key
S2356
Generate shared intermediate key
S2357
Obtain shared key
S2358
Output shared key to output unit
S2359
Output shared key to outside
Processing end

FIG. 51

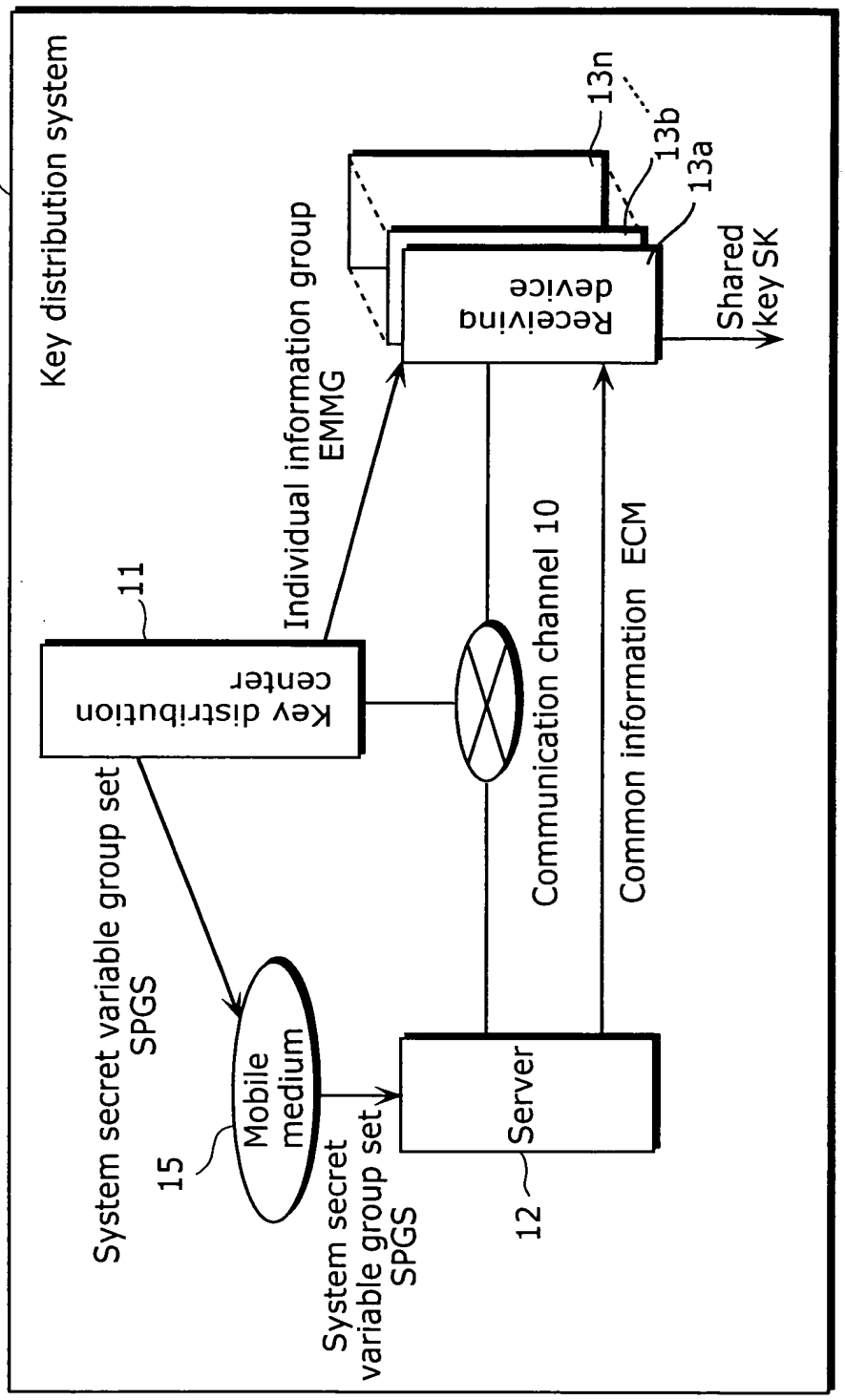

1
Key distribution system
11
Key distribution center
Individual information group EMMG
13n
13b
13a
Receiving device
Shared key SK
Communication channel 10
Common information ECM
System secret variable group set SPGS
15
Mobile medium
System secret variable group set SPGS
12
Server

FIG. 52

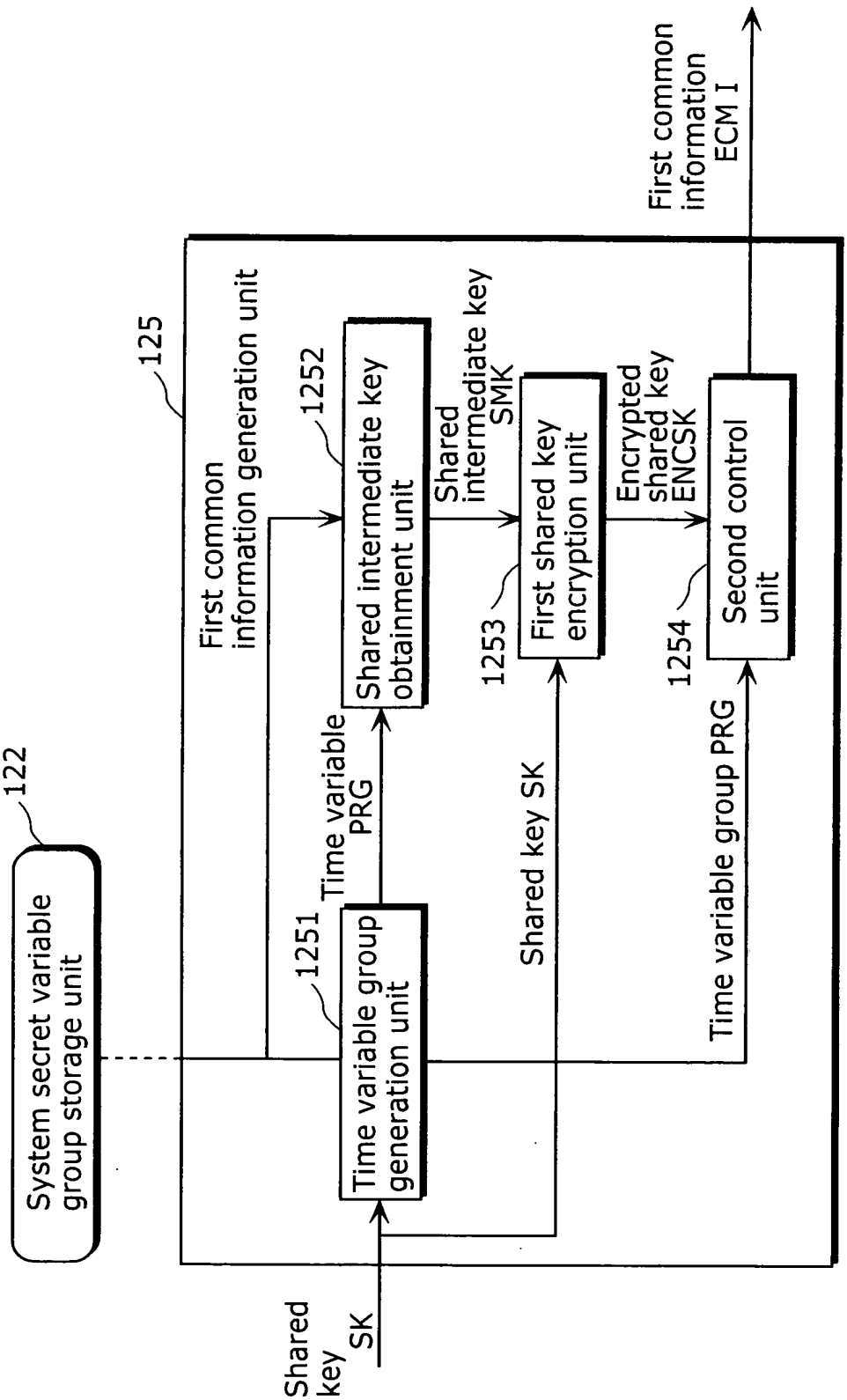
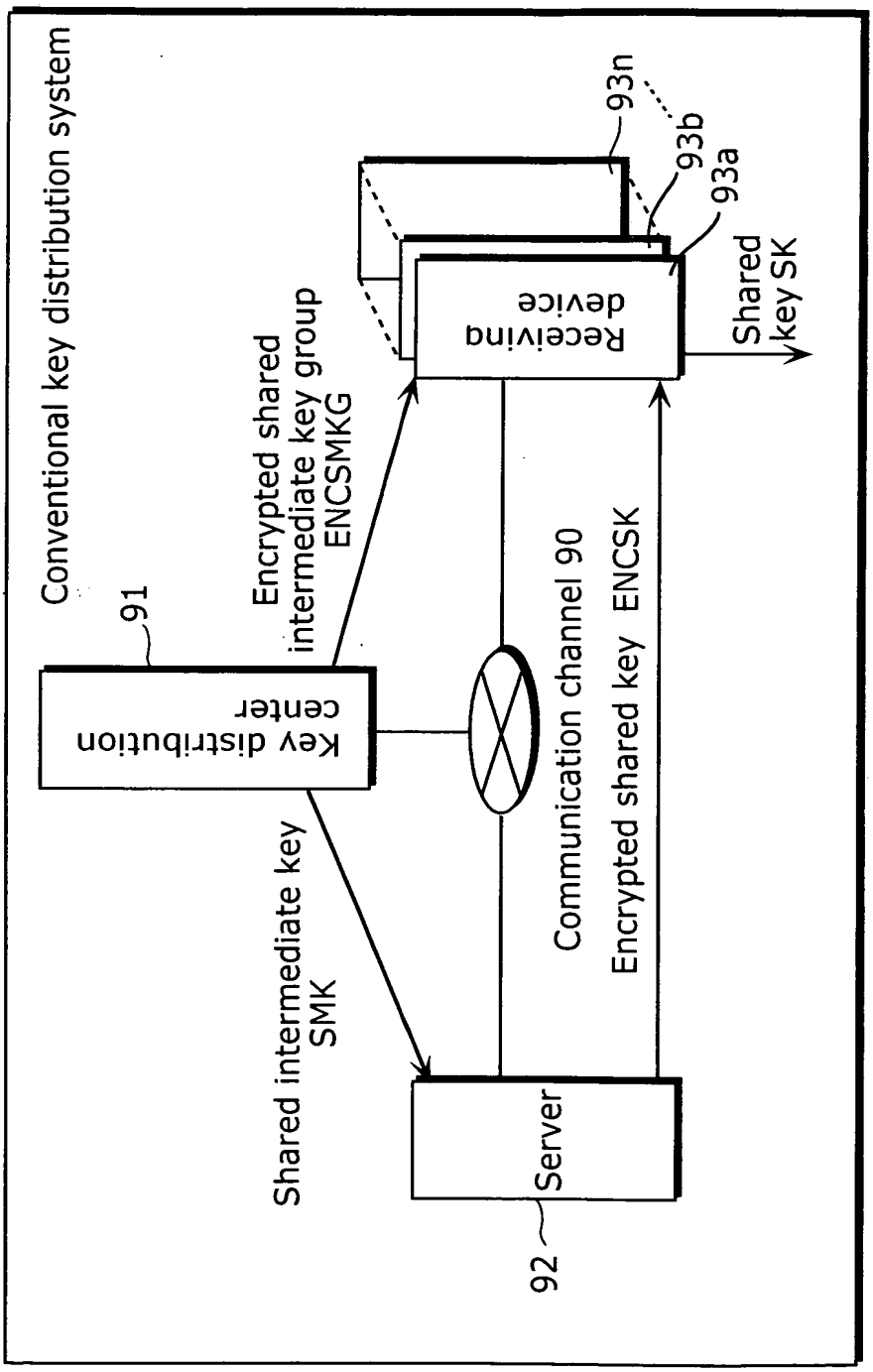

122
System secret variable group storage unit
125
First common information generation unit
1251
Time variable group generation unit
Time variable PRG
1252
Shared intermediate key obtainment unit
Shared intermediate key SMK
1253
First shared key encryption unit
Encrypted shared key ENCSK
1254
Second control unit
First common information ECM I
Shared key SK
Shared key SK
Time variable group PRG

FIG. 53


Conventional key distribution system
91
Key distribution center
Encrypted shared intermediate key group ENCSMKG
Shared intermediate key SMK
Communication channel 90
Encrypted shared key ENCSK
Server
92
Receiving device
93a
93b
93n
Shared key SK